LPB2810A
LPB2826A
LPB2848A

PoE+ Gigabit Managed Switch Eco

User Manual

An affordable managed switch with the power to be a key component of your network infrastructure.

Customer Support Information

Order toll-free in the U.S.: Call 877-877-BBOX (outside U.S. call 724-746-5500)
FREE technical support 24 hours a day, 7 days a week: Call 724-746-5500 or fax 724-746-0746
Mailing address: Black Box Corporation, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: www.blackbox.com • E-mail: info@blackbox.com

Trademarks Used in this Manual

Black Box and the Double Diamond logo are registered trademarks of BB Technologies, Inc.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

We're here to help! If you have any questions about your application
or our products, contact Black Box Tech Support at **724-746-5500**
or go to **blackbox.com** and click on "Talk to Black Box."
You'll be live with one of our technical experts in less than 30 seconds.

Federal Communications Commission and Industry Canada Radio Frequency Interference Statements

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

Instrucciones de Seguridad
(Normas Oficiales Mexicanas Electrical Safety Statement)

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
    - A: El cable de poder o el contacto ha sido dañado; u
    - B: Objectos han caído o líquido ha sido derramado dentro del aparato; o
    - C: El aparato ha sido expuesto a la lluvia; o
    - D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
    - E: El aparato ha sido tirado o su cubierta ha sido dañada.

Table of Contents

1. Overview 9
1.1 Initial Configuration 10
1.2 Connecting to PCs, Servers, Hubs, and Switches 13
1.3 Network Wiring Connections 14

2. System Configuration 15
2.1 System Information 15
2.1.1 Information 15
2.1.2 Configuration 17
2.1.3 CPU Load 18
2.2 Time 19
2.2.1 Manual 19
2.2.2 NTP 21
2.3 Account 21
2.3.1 Users 22
2.3.2 Privilege Levels 23
2.4 IP (Internet Protocol) 25
2.4.1 IPv4 25
2.4.2 IPV6 27
2.5 Syslog 28
2.5.1 Configuration 28
2.5.2 Log 29
2.5.3 Detailed Log 30
2.6 SNMP 31
2.6.1 System 31
2.6.2 Communities 32
2.6.3 Users 33
2.6.4 Groups 35
2.6.5 Views 36
2.6.6 Access 37
2.6.7 Trap 38

3. Configuration 40
3.1 Port 40
3.1.1 Configuration 40
3.1.2 Port Description 42
3.1.3 Traffic Overview 43
3.1.4 Detailed Statistics 44
3.1.5 Qos Statistics 46
3.1.6 SFP Information 47
3.1.7 EEE 48
3.2 ACL 50
3.2.1 Ports 50
3.2.2 Rate Limiters 52
3.2.3 Access Control List 53
3.2.4 ACL Status 55
3.3 Aggregation 57
3.3.1 Static Trunk 57
3.3.2 LACP 59

3.4 Spanning Tree 63
3.4.1 Bridge Settings 64
3.4.2. MSTI Mapping 65
3.4.3 MSTI Priorities 66
3.4.4 CIST Ports 67
3.4.5 MSTI Ports 69
3.4.6 Bridge Status 70
3.4.7 Port Status 71
3.4.8 Port Statistics 72
3.5 Loop Detection 73
3.6 IGMP Snooping 74
3.6.1 Basic Configuration 74
3.6.2 VLAN Configuration 75
3.6.3 Port Group Filtering 76
3.6.4 Status 78
3.6.5 Group Information 79
3.6.6 IPv4 SSM information 80
3.7 MLD Snooping 82
3.7.1 Basic Configuration 82
3.7.2 VLAN Configuration 84
3.7.3 Port Group Filtering 85
3.7.4 Status 86
3.7.5 Group Information 87
3.7.6 IPv6 SSM Information 88
3.8 MVR 89
3.8.1 Configuration 89
3.8.2 Groups Information 90
3.8.3 Statistics 91
3.9 LLDP 92
3.9.1 LLDP Configuration 92
3.9.2 LLDP Neighbors 94
3.9.3 LLDP-MED Configuration 95
3.9.4 LLDP-MED Neighbors 100
3.9.5 PoE 103
3.9.6 EEE 104
3.9.7 Port Statistics 105
3.10 PoE 107
3.10.1 Configuration 107
3.10.2 Status 108
3.11 Filtering Data Base 109
3.11.1 Configuration 109
3.11.2 Dynamic MAC Table 112
3.12 VLAN 113
3.12.1 VLAN Membership 114
3.12.2 Ports 115
3.12.3 Switch Status 117
3.12.4 Port Status 118
3.12.5 Private VLANs 119
3.12.6 MAC-Based VLAN 121
3.12.7 Protocol-Based VLAN 124
3.13 Voice VLAN 127

3.13.1 Configuration 127
3.13.2 OUI 129
3.14 GARP 130
3.14.1 Configuration 130
3.14.2 Statistics 132
3.15 GVRP 133
3.15.1 Configuration 133
3.15.2 Statistics 135
3.16 QoS 136
3.16.1 Port Classification 136
3.16.2 Port Policing 137
3.16.3 Port Scheduler 139
3.16.4 Port Shaping 141
3.16.5 Port Tag Remarking 143
3.16.6 Port DSCP 144
3.16.7 DSCP-Based QoS 145
3.16.8 DSCP Translation 147
3.16.9 DSCP Classification 149
3.16.10 QoS Control List Configuration 150
3.16.11 QCL Status 153
3.16.12 Storm Control 154
3.17 Thermal Protection 155
3.17.1 Configuration 155
3.17.2 Status 156
3.18 sFlow Agent 157
3.18.1 sFlow Collector 157
3.18.2 Sampler 158
3.19 Loop Protection 160
3.19.1 Configuration 160
3.19.2 Status 161
3.20 Single IP 162
3.21 Easy Port 164
3.22 Mirroring 166
3.23 Trap Event Severity 167
3.24 SMTP Configuration 168
3.25 UPnP 169

4. Security 170
4.1. IP Source Guard 170
4.1.1 Configuration 170
4.1.2 Static Table 171
4.1.3 Dynamic Table 172
4.2 ARP Inspection 173
4.2.1 Configuration 173
4.2.2 Static Table 174
4.2.3 Dynamic Table 175
4.3 DHCP Snooping 176
4.3.1 Configuration 176
4.3.2 Statistics 177
4.4 DHCP Relay 178
4.4.1 Configuration 178

4.4.2 Statistics 179
4.5 NAS 181
4.5.1 Configuration 181
4.5.2 Switch Status 187
4.5.3 Port Status 188
4.6 AAA 190
4.6.1 Configuration 190
4.6.2 RADIUS Overview 193
4.6.3 RADIUS Details 194
4.7 Port Security 195
4.7.1 Limit Control 195
4.7.2 Switch Status 197
4.7.3 Port Status 199
4.8 Access Management 200
4.8.1 Configuration 200
4.8.2 Statistics 201
4.9 SSH 202
4.10 HTTPS 203
4.11 Authentication Method 204
5. Maintenance 205
5.1 Restart Device 205
5.2 Firmware 206
5.2.1 Firmware Upgrade 206
5.2.2 Firmware Selection 207
5.3 Save / Restore 208
5.3.1 Factory Defaults 208
5.3.2 Save Start 209
5.3.3 Save User 209
5.3.4 Restore User 211
5.4 Export / Import 212
5.4.1 Export Config 212
5.4.2 Import Config 213
5.5 Diagnostics 214
5.5.1 Ping 214
5.5.2 Ping6 215
5.5.3 VeriPHY 216
Appendix: Glossary of Web-Based Management Terms 217

1. Overview

This user's manual provides step-by-step instructions for configuring and monitoring your PoE+ Gigabit Managed Switch Eco through the Web via an RJ-45 (serial) interface and Ethernet port. Detailed explanations of hardware and software functions are shown, along with examples of the operation for Web-based interface.

The PoE+ Gigabit Managed Switch Eco, part of the next generation of Web-managed switches from Black Box, provides a reliable infrastructure for your business network. This switch delivers the intelligent features you need to improve the availability of your critical business applications, to protect your sensitive information, and to optimize your network bandwidth to deliver information and applications more effectively. It provides the ideal combination of affordability and capabilities for entry-level networking. Whether you have a small business or enterprise application, this switch will enable you to create a more efficient, better-connected workforce.

The PoE+ Gigabit Managed Switch Eco provides 10, 26, or 48 ports in a single device. Its features include:

- L2+ features provide better manageability, security, QoS, and performance.
- High port count design with all Gigabit Ethernet ports.
- Supports guest VLAN, voice VLAN, port-based, tag-based and protocol-based VLANs.
- Supports 802.3az Energy Efficient Ethernet standards.
- Supports 8K MAC table.
- Supports IPv6/ IPv4 Dual stack.
- Supports s-Flow.
- Supports Easy-Configuration-Port for easy implementation in IP phone, IP camera, or wireless environments.

1.1 Initial Configuration

This section details how to configure and manage the PoE+ Gigabit Managed Switch Eco through the Web user interface. This feature enables administrators to easily access and monitor the entire status of the switch through any one port of the switch. Statuses which may be monitored include status of the MIBs, activity of each port, status of spanning trees, port aggregation status, multicast traffic, VLAN and priority status, even illegal access records.

The default values of the PoE+ Gigabit Managed Switch Eco are listed in the table below:

Table 1-1: Using Web-based management.

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default	192.168.1.254
Username	admin
Password	

After the PoE+ Gigabit Managed Switch Eco has been configured in the interface, you can browse it. For instance, type http://192.168.1.1 in the address row in a browser. You will see the screen in Figure 1-1, requesting your username and password to log in and authenticate your access.

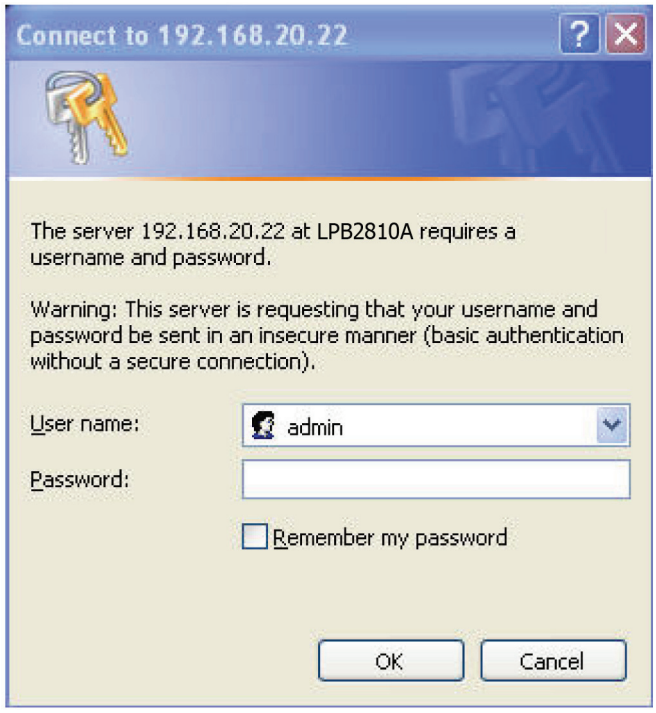


Figure 1-1. The login screen.

The default username is “admin” and password is empty. For the first use, please enter the default username and password, then click the <Login> button.

The login process now is completed. In this login menu, you must input the complete username and password respectively: the PoE+ Gigabit Managed Switch Eco will not give you a shortcut to username automatically. This may be inconvenient, but it is safer.

The PoE+ Gigabit Managed Switch Eco supports a simple user management function allowing only one administrator to configure the system at the same time. If there are two or more users using an administrator's identity, it will only allow the one who logs in first to configure the system. The rest of the users, even with an administrator's identity, can only monitor the system. Those who have no administrator's identity can only monitor the system. There is a maximum of three users able to login simultaneously in the PoE+ Gigabit Managed Switch Eco.

NOTE: When you log in to the Switch Web Manager, you must first type the Username of the admin. The password must remain blank at this point, so simply press Enter. When you log in the PoE+ Gigabit Managed Switch Eco Web UI management, you can use either an ipv4 or ipv6 log in. To optimize the display, we recommend you use Microsoft® Internet Explorer® 6.0 or higher, Netscape® V7.1 or higher, or FireFox® V1.00 above and set the resolution 1024x768. The switch supports a neutral Web browser interface.

NOTE: the PoE+ Gigabit Managed Switch Eco enables the DHCP function, so if you do not have DHCP server to provide IP addresses to the switch, the switch default IP is 192.168.1.1.

NOTE: If you need to configure the function or parameter, refer to those sections in the User Guide. Or, access the switch and click the "help" under the Web GUI, and the switch will open its easy-to-use help content to teach you how to set the parameters, as shown in Figure 1-2.

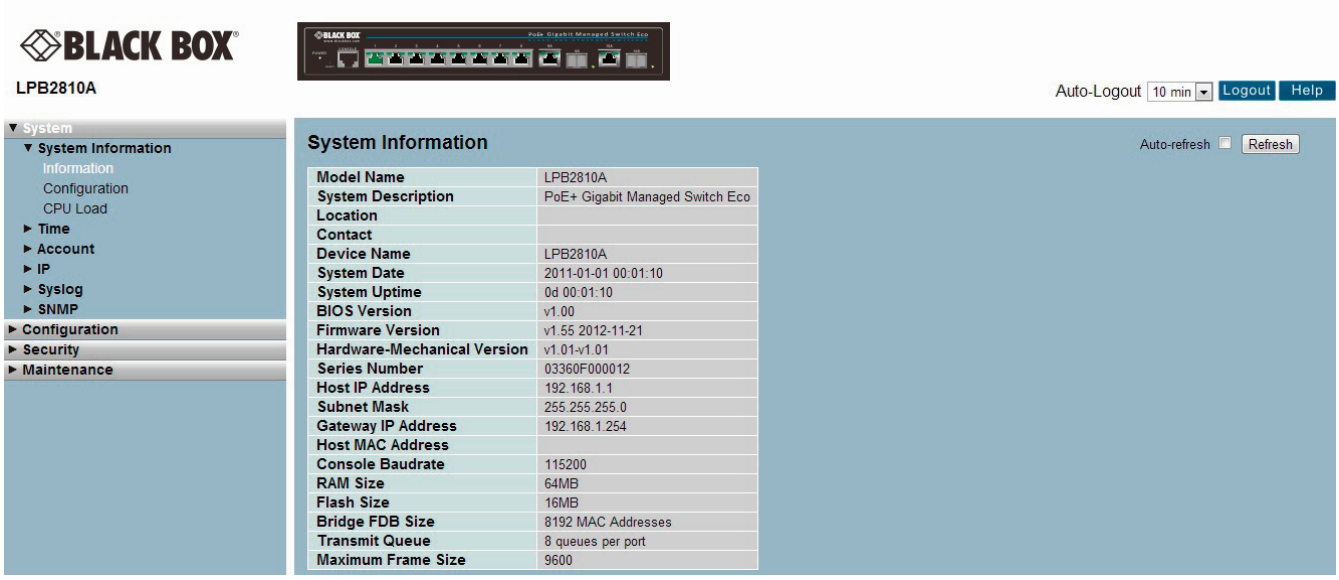


Figure 1-2. Accessing the on-line help function.

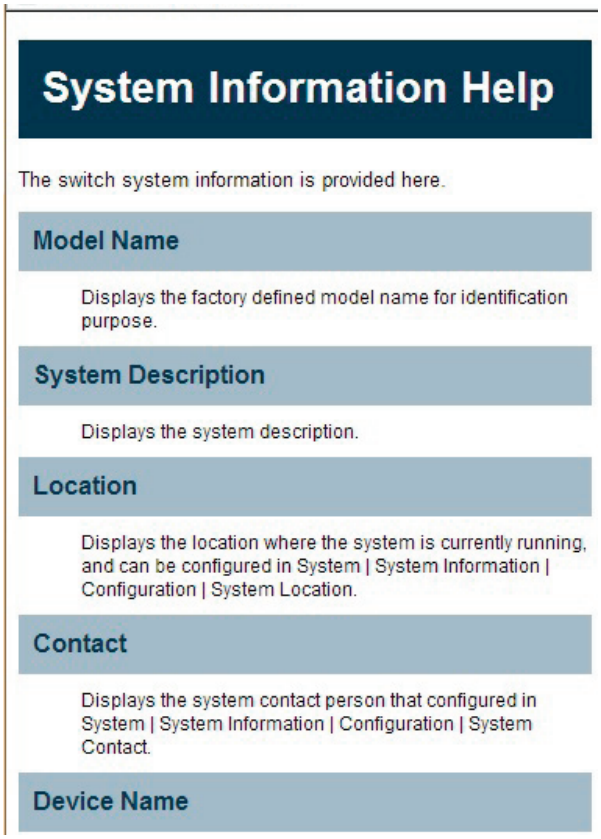


Figure 1-2 (Continued). Accessing the on-line help function.

Connecting Network Devices

The switch is designed to be connected to 10-, 100-, or 1000-Mbps network cards in PCs and servers, as well as to other switches and hubs. It may also be connected to remote devices using optional SFP transceivers.

Twisted-Pair Devices

Each device requires an unshielded twisted-pair (UTP) cable with RJ-45 connectors at both ends. Use Category 5, 5e, or 6 cable for 1000BASE-T connections, Category 5 or better for 100BASE-TX connections.

Cabling Guidelines

The RJ-45 ports on the switch support automatic MDI/MDI-X pinout configuration, so you can use standard straight-through twisted-pair cables to connect to any other network device (PCs, servers, switches, routers, or hubs).

See Section 4.2 of the LPB2810A Quick Start Guide, "Ethernet Cabling," for more information on cabling.

CAUTION: Do not plug a phone jack connector into an RJ-45 port. This will damage the switch. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

1.2 Connecting to PCs, Servers, Hubs, and Switches

Step 1: Attach one end of a twisted-pair cable segment to the device's RJ-45 connector.

Step 2. If the device is a network card and the switch is in the wiring closet, attach the other end of the cable segment to a modular wall outlet that is connected to the wiring closet. (See Section 1.3, "Network Wiring Connections.") Otherwise, attach the other end to an available port on the switch. Make sure each twisted-pair cable does not exceed 328 feet (100 m) in length.

NOTE: Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise backpressure jamming signals may degrade overall performance for the segment attached to the hub.

Step 3. As each connection is made, the Link LED (on the switch) corresponding to each port will light green (1000 Mbps) or amber (100 Mbps) to indicate that the connection is valid.

1.3 Network Wiring Connections

Today, the punchdown block is an integral part of many of the newer equipment racks. It is actually part of the patch panel. Instructions for making connections in the wiring closet with this type of equipment follows:

Step 1: Attach one end of a patch cable to an available port on the switch, and the other end to the patch panel.

Step 2. If not already in place, attach one end of a cable segment to the back of the patch panel where the punchdown block is located, and the other end to a modular wall outlet.

Step 3. Label the cables to simplify future troubleshooting. See Chapter 6 of the PoE+ Gigabit Managed Switch Eco Quick Start Guide: "Labeling Connections."

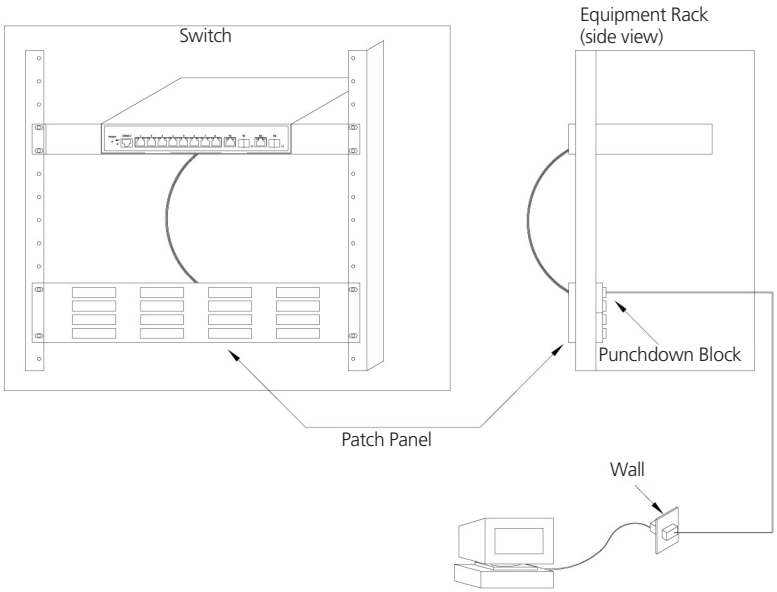


Figure 1-3. Network wiring connections.

2. System Configuration

This chapter describes all of the basic configration tasks, including the system information and any management of the switch (e.g., Time, Account, IP, Syslog, and SNMP).

2.1 System Information

After logging in, the switch shows you the system information. This page is the default and tells you the basic information of the system, including "Model Name", "System Description", "Contact", "Device Name", "System Uptime", "BIOS Version", "Firmware Version", "Hardware-Mechanical Version", "Serial Number", "Host IP Address", "Host Mac Address", "Device Port", "RAM Size" , "Flash Size" etc. With this information, you will know the software version used, MAC address, serial number, how many ports good and so on, information you will need for troubleshooting or when contacting Tech Support.

2.1.1 Information

The switch system information is provided here.

Web interface

To configure System Information in the Web interface:

1. Click SYSTEM, System, and Information.
2. Specify the contact information for the system administrator as well as the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset.
3. Click Refresh.

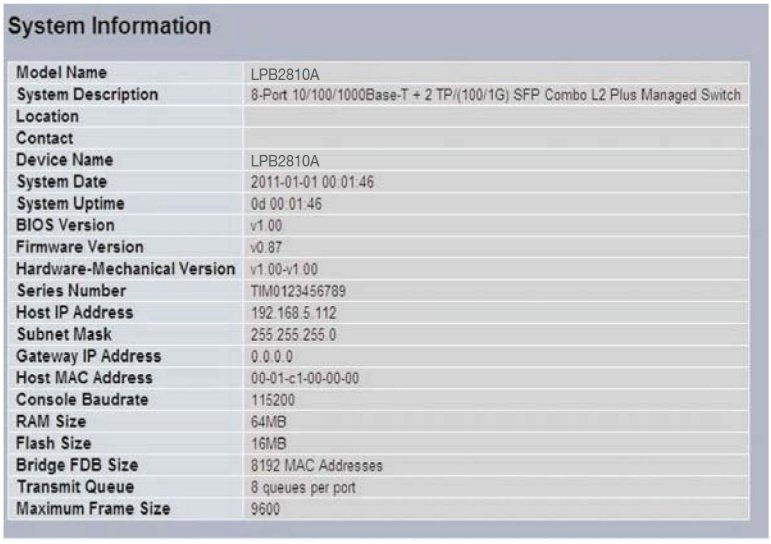


Figure 2-1. System Information screen.

Parameter Description

- **Model Name**: The model name of this device.
- **System Description**: This tells what this device is. Here, it is "8 port 10/100/1000 Base-T + 2-Port Dual Personality (RJ-45/SFP) Web Managed Switch".
- **Location**: This is the location where this switch is put. User-defined.

- **Contact**: Enter the contact person's name and phone here. You can configure this parameter through the device's user interface or SNMP.
- **Device Name**: The name of the switch. User-defined.
- **System Date**: Show the system time of the switch. Its format: day of week, month, day, hours : minutes : seconds, year.
- **System Uptime**: The time accumulated since this switch is powered up. Its format is day, hour, minute, second.
- **BIOS Version**: The version of the BIOS in this switch.
- **Firmware Version**: The firmware version in this switch.
- **Hardware-Mechanical Version**: The figure before the hyphen is the version of electronic hardware; the one after the hyphen is the mechanical version.
- **Serial Number**: The serial number is assigned by the manufacturer.
- **Host IP Address**: The IP address of the switch.
- **Host MAC Address**: It is the Ethernet MAC address of the management agent in this switch.
- **Device Port**: Show all types and numbers of the port in the switch.
- **RAM Size**: The size of the RAM in this switch.
- **Flash Size**: The size of the flash memory in this switch.
- **Bridge FDB Size**: Displays the bridge FDB size information.
- **Transmit Queue** : Displays the device's transmit hardware priority queue information.
- **Maximum Frame Size**: Displays the device's maximum frame size information.

2.1.2 Configuration

You can identify the system by configuring the contact information, name, and location of the switch.

Web Interface

To configure System Information in the Web interface:

1. Click System, System Information, Configuration.
2. Write System Contact, System Name, System Location information in this page.
3. Click Save.

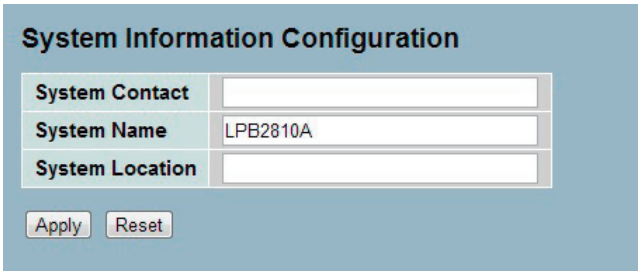


Figure 2-2. System Information Configuration screen.

Parameter Description

- **System Contact**: The textual identification of the contact person for this managed node, together with information on how to contact this person. The string length should be 0 to 255 characters, and the type of content permitted is the ASCII characters from 32 to 126.
- **System Name**: An administratively assigned name for this managed node. By convention, this is the node's fully qualified domain name. A domain name is a text string drawn from letters (A-Z, a-z), numbers (0-9), and the minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The string length should be 0 to 255.
- **System Location**: Describes the physical location of this node (e.g., telephone closet, 3rd floor). The string length should be 0 to 255 characters, and the content should be ASCII characters from 32 to 126.

2.1.3 CPU Load

This page displays the CPU load, using an SVG graph. The load is measured as averaged over the last 100-ms, 1-second, and 10-second intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. To display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plug-in installed to support SVG.

Web Interface

To configure System Information in the Web interface:

1. Click System, System Information, CPU Load.
2. Display the CPU Load on the screen.
3. Click Auto-refresh.

Figure 2-3: CPU Load screen.

Parameter Description

• To set the switch to auto-refresh the log, check "Auto-refresh."

NOTE: The screen under "from" and "to" will display what you set on the "From" and "To" field information.

2.2 Time

This section describes how to configure the switch time, including Time Configuration and NTP Configuration.

2.2.1 Manual

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple. Input "Year", "Month", "Day", "Hour", "Minute" and "Second" within the valid value range indicated in each item.

Web Interface

To configure Time in the Web interface:

1. Click Time, Manual.
2. Specify the Time parameter in manual parameters.
3. Click Save.

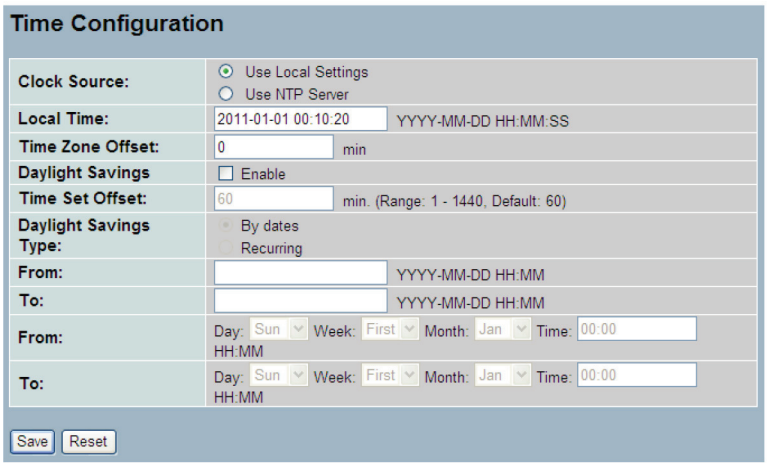


Figure 2-4: The time configuration screen.

Parameter Description

- **Clock Source**: Select which clock source to use for the PoE+ Gigabit Managed Switch Eco. You can select "Use local Settings" or "Use NTP Server."
- **Local Time**: Show the current time of the system.
- **Time Zone Offset**: Provides the time zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.

- **Daylight Savings**: Daylight savings time is used in some countries. If you select this setting, the unit will adjust the time, forward or backward in increments of one hour, between the starting date and the ending date that you select. For example, if you set the daylight savings offset to be 1 hour, when the time reaches the starting time, the system time will be increased one hour. And when the time reaches the ending time, the system time will be decreased one hour.

  The switch supports valid configurable daylight savings times of –5 to +5 hours in one-hour increments. The zero for this parameter means you will not have to adjust the current time to enact daylight saving. However, remember that if you do set the unit to observe daylight savings time, you will need to set the starting/ending date as well. If you do not set the start/end dates, the daylight savings function will not be activated.
- **Time Set Offset:** Provide the daylight saving time set offset in this space. The offset is given in minutes east of GMT. The valid range is from 1 to 1440 minutes. The default is 60 minutes.
- **Daylight Savings Type**: Provide the daylight savings type selection. You can select "By Dates" or "Recurring" type for Daylight saving type.
- **From**: To configure when daylight savings start date and time, the format is "YYYY-MMDD HH:MM".
- **To**: To configure when daylight savings end date and time, the format is "YYYY-MMDD HH:MM".

NOTE: The under "from" and "to" was displayed what you set on the "From" and "To" field information.

2.2.2 NTP

NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If you use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will sync the time a short time after pressing yjr <Apply> button. Although it synchronizes the time automatically, NTP does not update the time periodically without user input.

Time Zone is an offset time of GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and the updated NTP time to calculate the local time; otherwise, you will not able to get the correct time. The switch supports configurable time zones from –12 to +13 step in one-hour increments.

Default Time zone: +8 Hrs.

Web Interface

To configure Time in the Web interface:

1. Click SYSTEM, NTP.
2. Specify the Time parameter in manual parameters.
3. Click Save.

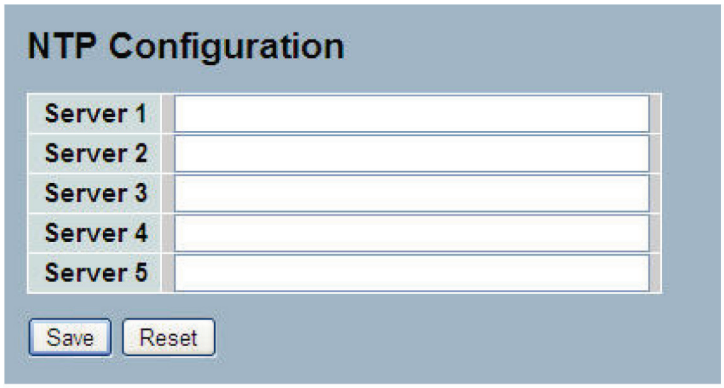


Figure 2-5: The NTP configuration screen.

Parameter Description

- **Server 1 to 5**: Provide the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, in "fe80::215:c5ff:fe03:4dc7", the symbol "::" is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, "::192.1.2.34".
- **Buttons**: These buttons are displayed on the NTP page:
  - Save: Click to save changes
  - Reset: Click to undo any changes made locally and revert to previously saved values.

2.3 Account

Only an administrator can create, modify, or delete the username and password. An administrator can modify other guest identities' passwords without confirming the password, but it is necessary to modify the administrator-equivalent identity. A Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field "Authorization in advance" before configuring the username and password. Only one administrator is permitted to exist and is unable to be deleted. In addition, up to 4 guest accounts may be created.

2.3.1 Users

This page provides an overview of the current users. Currently the only way to log in as another user on the Web server is to close and reopen the browser.

Web Interface

To configure Account in the Web interface:

1. Click SYSTEM, Account, Users.
2. Click Add new user
3. Specify the User Name parameter.
4. Click Save.

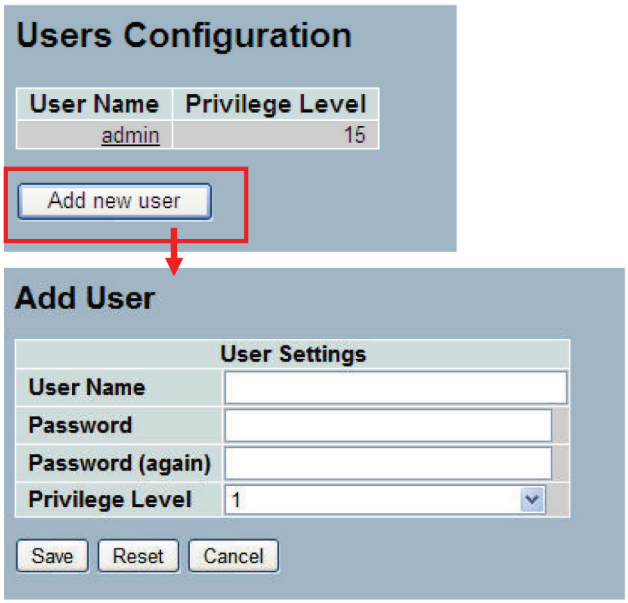


Figure 2-6. The Users Account configuration screen.

Parameter Description

- **User Name**: The name identifying the user. This is also a link to Add/Edit User.
- **Password**: To type the password. The specified string length is 0 to 255, and the specified content may include ASCII characters from 32 to 126.
- **Password (again)**: To type the password again. You must type the same password again in the field.
- **Privilege Level**: The privilege level of the user. The range is 1 to 15. A privilege level value of 15 may access all groups, i.e. it is a privilege level that is granted the full control of the device. For other users, the privilege level should be the same as or greater than the group privilege level to have the access of that group. By default setting, most groups will have a privilege level 5, granting read-only access; a privilege level of 10 has the read-write access. For system maintenance (software uploads, factory defaults and etc.) users will need to have a user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

2.3.2 Privilege Levels

This section provides an overview of Privilege Levels. The switch enables administrators to set user privileges in a number of different categories, including Account, Aggregation, Diagnostics, EEE, GARP, GVRP, IP, IPMC, Snooping, LACP, LLDP, LLDP, MED, MAC, Table, MRP, MVR, MVRP, Maintenance, Mirroring, PoE, Ports, Private VLANs, QoS, SMTP, SNMP, Security, Spanning Tree, System, Trap Event ,VCL, VLANs, and Voice VLAN Privilege Levels from 1 to 15.

Web Interface

To configure Privilege Level in the Web interface:

1. Click SYSTEM, Account, Privilege Level.
2. Specify the Privilege parameter.
3. Click Save.

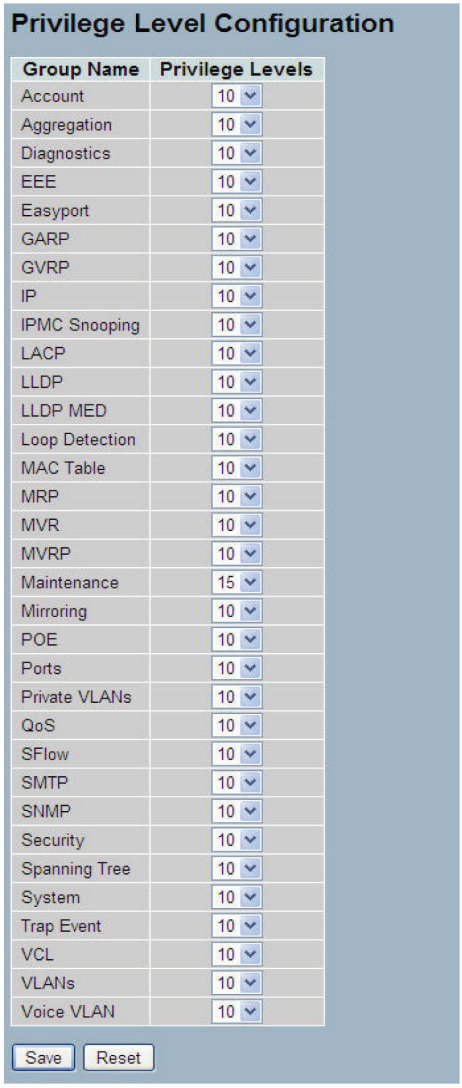


Figure 2-7. The Privilege Level Configuration screen.

Parameter Description

- Group Name

  The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contain more than one. The following description defines these privilege level groups in detail:

  - System: Contact, Name, Location, Timezone, Log.

  - Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard.

  - IP: Everything except 'ping'.

  - Port: Everything except 'VeriPHY'.

  - Diagnostics: 'ping' and 'VeriPHY'.

  - Maintenance: System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load, Web users, Privilege Levels, and everything in Maintenance.

- Privilege Levels

  Every group has an authorization Privilege Level for the following subgroups: configuration read-only; configuration/execute read-write; status/statistics read-only; status/statistics read-write (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

2.4 IP (Internet Protocol)

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an Internet network.

IP is a "best effort" system, which means that no packet of information sent over is ensured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of Webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

2.4.1 IPv4

The IPv4 address for the switch could be obtained via DHCP Server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

Configure the switch-managed IP information on this page.

The Configured column is used to view or change the IP configuration.

The Current column is used to show the active IP configuration.

Web Interface

To configure an IP address in the Web interface:

1. Click System, IP Configuration.
2. Specify the IPv4 settings, and enable DNS proxy service if required.
3. Click Save.

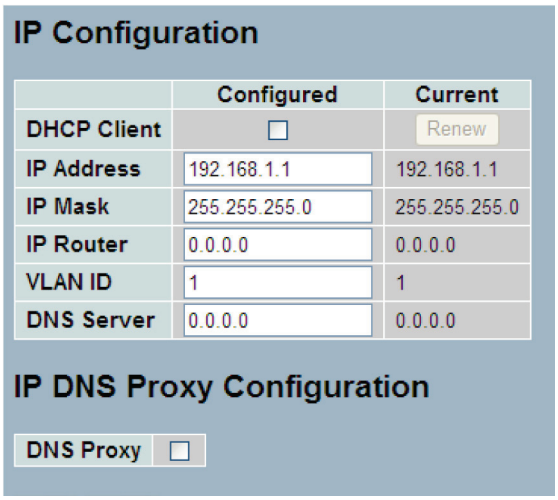


Figure 2-8. The IP Configuration screen.

Parameter Description

- **DHCP Client**: Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured system name as hostname to provide DNS lookup.
- **IP Address**: Provide the IP address of this switch in dotted decimal notation.
- **IP Mask**: Provide the IP mask of this switch dotted decimal notation.
- **IP Router**: Provide the IP address of the router in dotted decimal notation.
- **SNTP Server**: Provide the IP address of the SNTP Server in dotted decimal notation.
- **DNS Server**: Provide the IP address of the DNS Server in dotted decimal notation.
- **VLAN ID**: Provide the managed VLAN ID. The permitted range is 1 to 4095.
- **DNS Proxy**: When DNS proxy is enabled, DUT will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client device on the network.

2.4.2 IPV6

This section describes how to configure the switch-managed IPv6 information. The Configured column is used to view or change the IPv6 configuration. And the Current column is used to show the active IPv6 configuration.

Configure the switch-managed IPv6 information on this page.

The Configured column is used to view or change the IPv6 configuration.

The Current column is used to show the active IPv6 configuration.

Web Interface

To configure Management IPv6 of the switch in the Web interface:

1. Click System, IPv6 Configuration.
2. Specify the IPv6 settings, and enable Auto Configuration service if required.
3. Click Save.

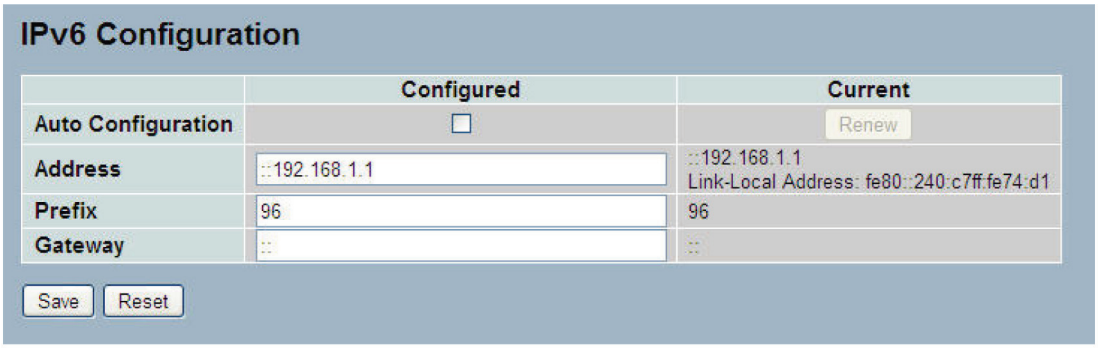


Figure 2-9. The IPv6 Configuration screen.

Parameter Description

- **Auto Configuration**: Enable IPv6 auto-configuration by checking this box. If fails, the configured IPv6 address is zero. The r outer may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.
- **Address**: Provide the IPv6 address of this switch. IPv6 address is represented in 128-bit records as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, in "fe80::215:c5ff:fe03:4dc7", the symbol "::" is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, "::192.1.2.34".
- **Prefix**: Provide the IPv6 Prefix of this switch. The range is 1 to 128.
- **Router**: Provide the IPv6 gateway address of this switch. IPv6 address is represented in 128-bit records as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, in "fe80::215:c5ff:fe03:4dc7", the symbol "::" is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, "::192.1.2.34".

2.5 Syslog

The Syslog (system log) is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can also be used for generalized informational, analysis, and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

2.5.1 Configuration

This section describes how to configure the system log and provide a wide variety of devices and receivers across multiple platforms.

Web Interface

To configure syslog configuration in the Web interface:

1. Click SYSTEM, Syslog.
2. Specify the syslog parameters including the IP address of the Syslog server and the port number.
3. Evoke the syslog to enable it.
4. Click Save.

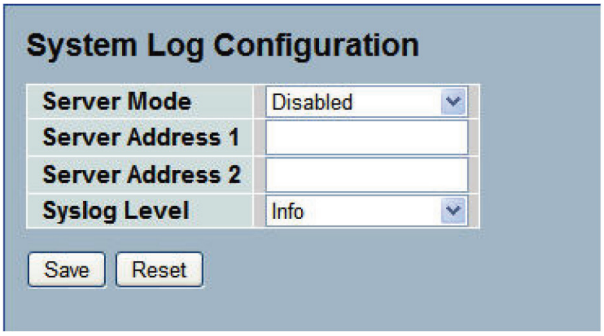


Figure 2-10. The System Log Configuration screen.

Parameter Description

- **Server Mode**: Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP Port 514. The syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always be sent out even if the syslog server does not exist. Possible modes are:
  - Enabled: Enable server mode operation.
  - Disabled: Disable server mode operation.
- **Server Address 1 and 2**: Indicates the IPv4 host address of syslog server 1 and server 2 (for redundancy). If the switch provides a DNS feature, it also can be a host name.
- **Syslog Level**: Indicates what kind of message it will send to the syslog server. Possible modes are:
  - Info: Send information, warnings, and errors.
  - Warning: Send warnings and errors.
  - Error: Send errors.

2.5.2 Log

This section describes how to display the System Log Information for the switch.

Web Interface

To display the log configuration in the Web interface:

1. Click Syslog, Log.
2. Display the log information.

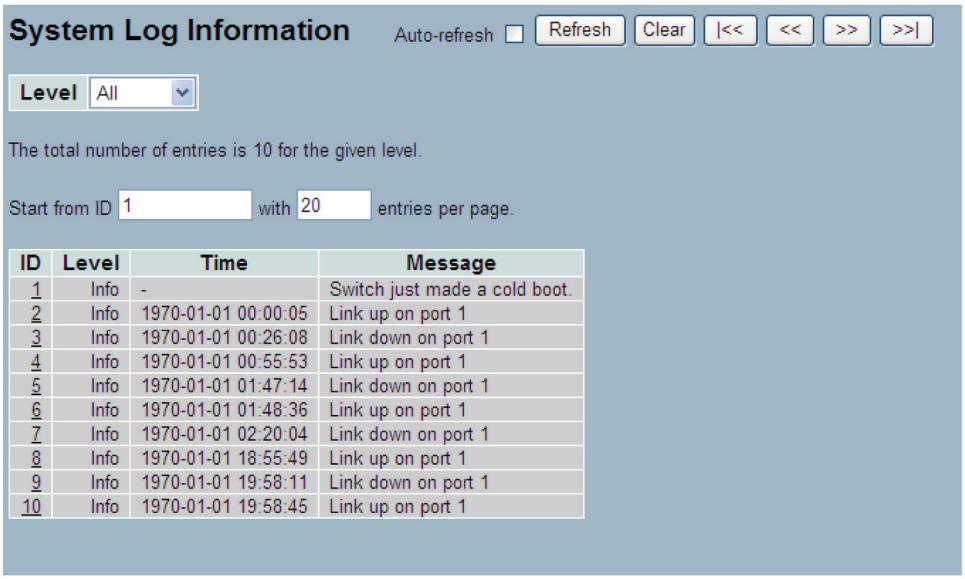


Figure 2-11. The System Log Information screen.

Parameter Description

- **Auto-refresh**: To set the switch to auto-refresh the log information, check "Auto-refresh."
- **Level**: level of the system log entry. The following level types are supported:
  - Information level of the system log.
  - Warning: Warning level of the system log.
  - Error: Error level of the system log.
  - All: All levels.
- **ID**: ID (>= 1) of the system log entry.
- **Time**: It will display the log record by device time. The time of the system log entry.
- **Message**: It will display the log detail message. The message of the system log entry.
- **Icons, upper right of screen (Refresh, clear,….)**: Click these to refresh the system log or clear them manually. Arrow functions enable you to navigate to the first, prior, next, or last page.

2.5.3 Detailed Log

This section describes how to use the Detailed Log Information for the switch.

Web Interface

To display the detailed log configuration in the Web interface:

1. Click Syslog, Detailed Log.
2. Display the log information.

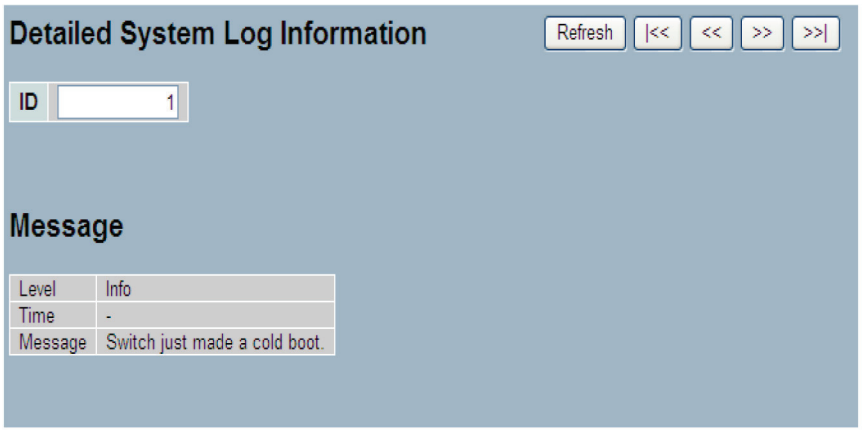


Figure 2-12. The Detailed System Log Information screen.

Parameter Description

- **ID**: The ID (>= 1) of the system log entry.
- **Message**: The detailed message of the system log entry.
- **Icons, upper right of screen (Refresh, clear, ….)**: Click to refresh the system log or to navigate to the first, prior, next, or last item.

2.6 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to responsd to the request issued by SNMP manager.

Essentially, SNMP is passive except for issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP "Enable", SNMP agent will start. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set "Disable," SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap, and all MIB counters will be ignored.

2.6.1 System

This section describes how to configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host, and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click the <Apply> button, and the setting takes effect.

Web Interface

To display the configure SNMP System in the Web interface:

1. Click SNMP, System.
2. Evoke SNMP State to enable or disable the SNMP function .
3. Specify the Engine ID
4. Click Apply.

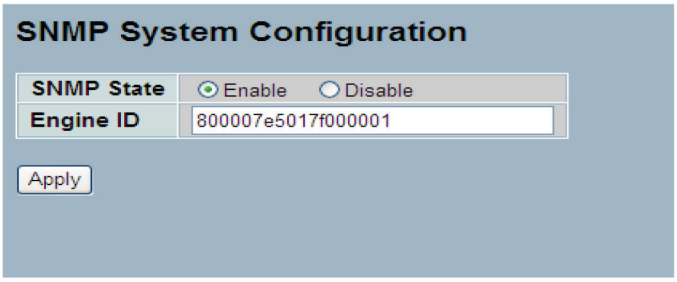


Figure 2-13. The SNMP System Configuration screen.

Parameter Description

These parameters are displayed on the SNMP System Configuration page:

- **SNMP State**: The term SNMP here is used for the activation or deactivation of SNMP.
  - Enable: Enable SNMP state operation.
  - Disable: Disable SNMP state operation.
  - Default: Enable.
- **Engine ID**: SNMPv3 engine ID. syntax: 0-9, a-f, A-F, min 5 octet, max 32 octet, fifth octet can't input 00. "Change the Engine ID" will clear all original users.

2.6.2 Communities

This function is used to configure SNMPv3 communities. The Community and UserName are unique. To create a new community account, check <Add new community> button, and enter the account information. Then click <Save>. The maximum group number is four.

Web Interface

To display the configure SNMP Communities in the Web interface:

1. Click SNMP, Communities.
2. Click Add new community.
3. Specify the SNMP communities parameters.
4. Click Save.
5. If you want to modify or clear the setting, then click Reset.

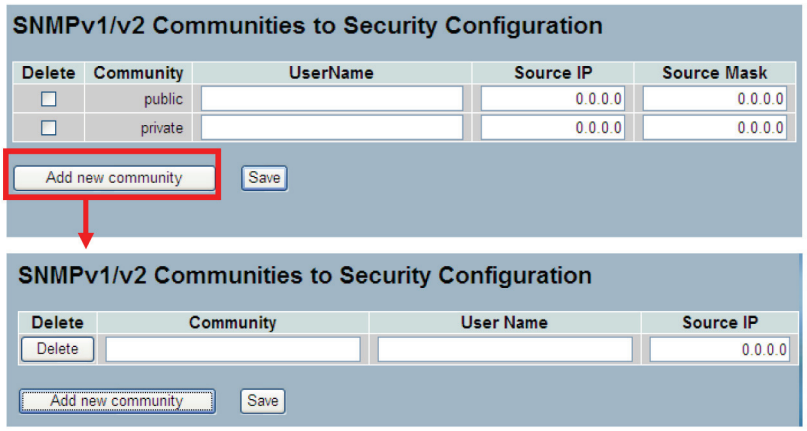


Figure 2-14. The SNMPv1/v2 Communities to Security Configuration screen.

Parameter Description

- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **Community**: Indicates the community access string to permit access to SNMPv3 agent. The string length should be 1 to 32 characters, using ASCII characters from 33 to 126. The community string will be treated as a security name and will map a SNMPv1 or SNMPv2c community string.
- **UserName**: The UserName access string to permit acccess to SNMPv3 agent. The "UserName" string is restricted to 1 to 32 characters.
- **Source IP**: Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
- **Source Mask**: Indicates the SNMP access source address mask.

2.6.3 Users

The function is used to configure SNMPv3 users. The Entry index key is UserName. To create a new UserName account, check the <Add new user> button, enter the user information, and then check <Save>. The maximum number of groups is 10.

Web Interface

To display the SNMP Users Configuration in the Web interface:

1. Click SNMP, Users.
2. Specify the Privilege parameter.
3. Click Save.

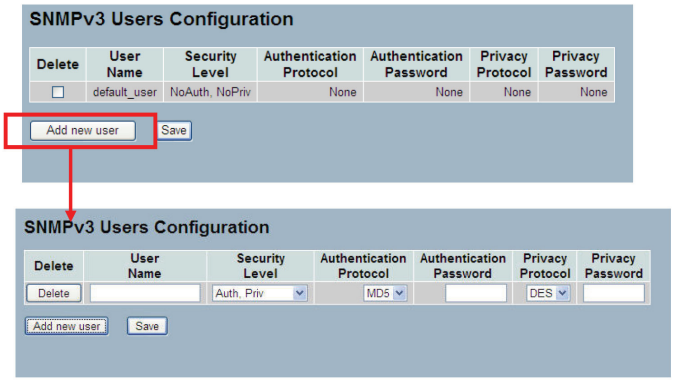


Figure 2-15. The SNMP Users Configuration screen.

Parameter Description

- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **User Name**: A string identifying the user name that this entry should belong to. The string length should be 1 to 32, characters, using ASCII characters from 33 to 126.
- **Security Level**: Indicates the security model that this entry should belong to. Possible security models are:
  - NoAuth, NoPriv: No authentication and no privacy.
  - Auth, NoPriv: Authentication and no privacy.
  - Auth, Priv: Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

- **Authentication Protocol**: Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:
  - None: No authentication protocol.
  - MD5: An optional flag to indicate that this user uses MD5 authentication protocol.
  - SHA: An optional flag to indicate that this user uses SHA authentication protocol.

The value of security level cannot be modified if an entry already exists. That means you must first make sure that the value is set correctly.

- **Authentication Password**: A string identifying the authentication password phrase. For MD5 authentication protocol, the string length should be 8 to 32 ASCII characters from 33 to 126. For SHA authentication protocol, the string length should 8 to 40ASCII characters from 33 to 126.
- **Privacy Protocol**: Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

  - None: No privacy protocol.

  - DES: An optional flag to indicate that this user uses DES authentication protocol.
- **Privacy Password**: A string identifying the privacy password phrase. The string length should be 8 to 32characters, using ASCII characters from 33 to 126.

2.6.4 Groups

This function is used to configure SNMPv3 group. The Entry index keys are Security Model and Security Name. To create a new group account, please check <Add new group> button, and enter the group information then check <Save>. The Maximum Group Number : v1: 2, v2: 2, v3:10.

Web Interface

To display the configure SNMP Groups in the Web interface:

1. Click SNMP, Groups.
2. Specify the Privilege parameter.
3. Click Save.

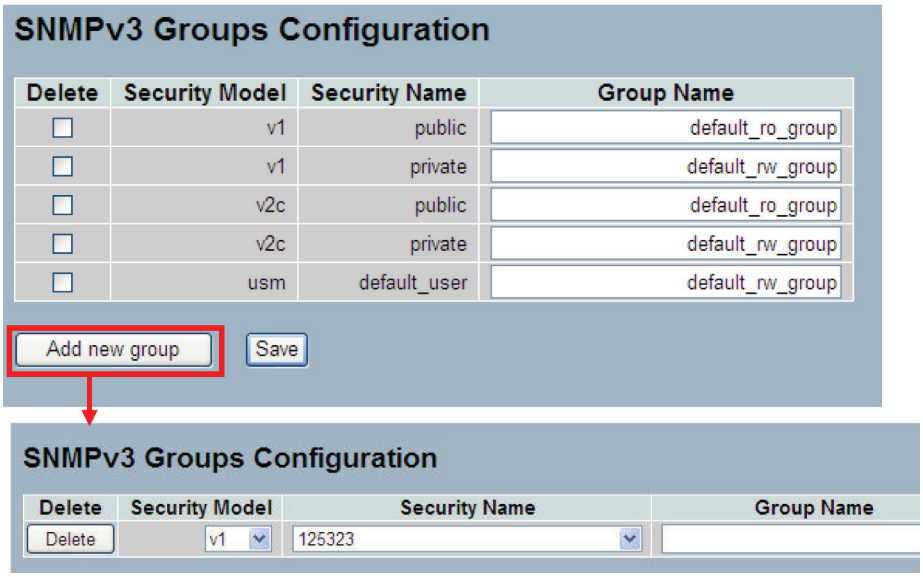


Figure 2-16. The SNMP Groups Configuration screen.

Parameter Description

- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **Security Model**: Indicates the security model that this entry should belong to. Possible security models are:
  - v1: Reserved for SNMPv1.
  - v2c: Reserved for SNMPv2c.
  - usm: User-based Security Model (USM).
- **Security Name**: A string identifying the security name that this entry should belong to. The string length should be 1 to 32 characters, using ASCII characters from 33 to 126.
- **Group Name**: A string identifying the group name that this entry should belong to. The string length should be 1 to 32 characters, using ASCII characters from 33 to 126.

2.6.5 Views

This function is used to configure SNMPv3 view. The entry index keys are OID Subtree and View Name. To create a new view account, click the <Add new view> button, and enter the view information then check <Save>. Max Group Number : 28.

Web Interface

1. Click SNMP, Views.
2. Click Add new View.
3. Specify the SNMP View parameters.
4. Click Save.
5. To modify or clear the setting, click Reset.

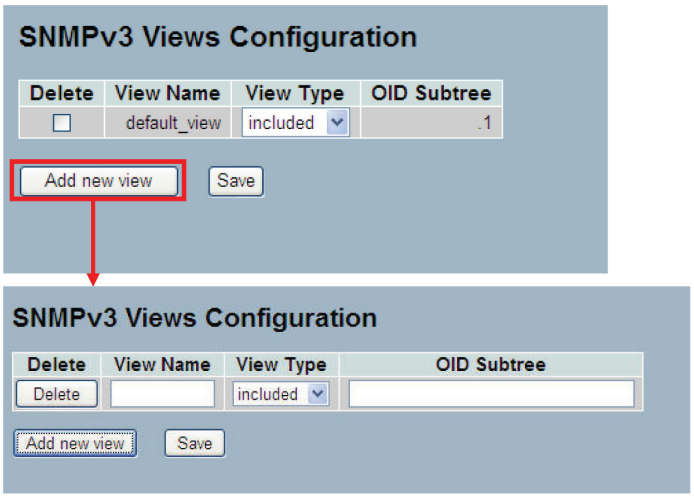


Figure 2-17. The SNMP Views Configuration screen.

Parameter Description

- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **View Name**: A string identifying the view name that this entry should belong to. The string length should be 1 to 32 characters, using ASCII characters from 33 to 126.
- **View Type**: Indicates the view type that this entry should belong to. Possible view types are:
  - Included: An optional flag to indicate that this view subtree should be included.
  - Excluded: An optional flag to indicate that this view subtree should be excluded.

In general, if a view entry's view type is "excluded," there should be another view entry existing with view type as "included" and its OID subtree should overstep the "excluded" view entry.

- **OID Subtree**: The OID defining the root of the subtree to add to the named view. The OID string length should be 1 to 128 characters., using only digital numbers or asterisks (*).
- **Save**: To click the Save icon to save the configuration to ROM.

2.6.6 Access

This function is used to configure SNMPv3 access. The entry index keys are Group Name, Security Model and Security level. To create a new access account, check <Add new access> button, and enter the access information then check <Save>. Max Group Number :14

Web Interface

To display the configure SNMP Access in the Web interface:

1. Click SNMP, Accesses.
2. Click Add new Access.
3. Specify the SNMP Access parameters.
4. Click Save.
5. To modify or clear the setting, click Reset.

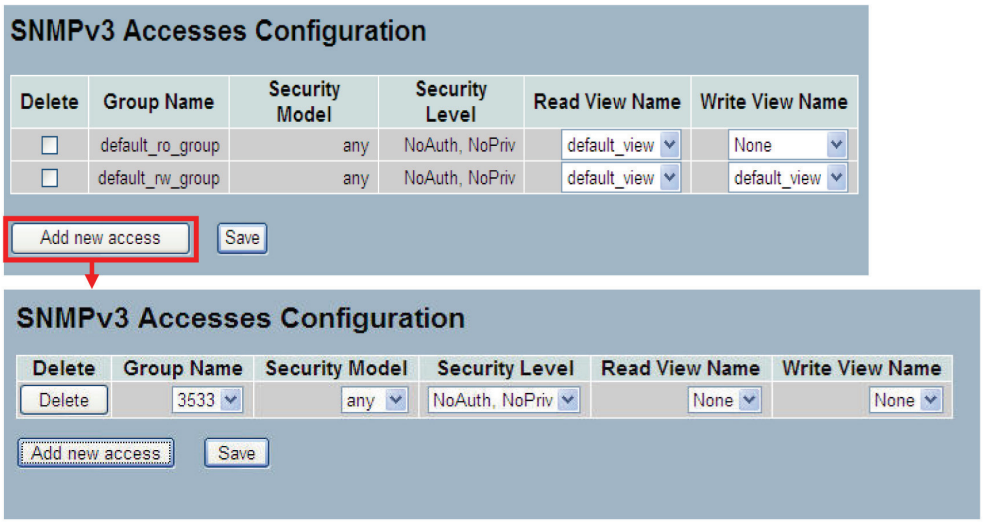


Figure 2-18. The SNMP Accesses Configuration screen.

Parameter Description

- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **Group Name**: A string identifying the group name that this entry should belong to. The string length should be 1 to 32 characters, using ASCII characters from 33 to 126.
- **Security Model**: Indicates the security model that this entry should belong to. Possible security models include:
  - any: Any security model accepted(v1|v2c|usm).
  - v1: Reserved for SNMPv1.
  - v2c: Reserved for SNMPv2c.
  - usm: User-based Security Model (USM).
- **Security Level**: Indicates the security level that this entry should belong to. Possible security levels are:
  - NoAuth, NoPriv: No authentication and no privacy.
  - Auth, NoPriv: Authentication and no privacy.
  - Auth, Priv: Authentication and privacy.

- **Read View Name**: The name of the MIB view defining the MIB objects for which this request may request the current values. The string length should be 1 to 32 characters, using ASCII characters from 33 to 126.
- **Write View Name**: The name of the MIB view defining the MIB objects for which this request may potentially set new values. The string length should be 1 to 32 characters, using ASCII characters from 33 to 126.

.

2.6.7 Trap

The function is used to configure SNMP trap. To create a new trap account, check <No number> button, and enter the trap information then check <Apply>. Max Group Number : 6.

Web Interface

To configure SNMP Trap setting:

1. Click SNMP, Trap.
2. Display the SNMP Trap Hosts information table.
3. Choose an entry to display and modify the detail parameters or click the Delete button to delete the trap hosts entry.

Figure 2-19. The SNMP Trap Host Configuration screen.

Parameters description:

- **Delete**: Check <Delete> entry then check <Save> button, the entry will be deleted.
- **Trap Version**: You may choose v1, v2c or v3 trap.
- **Server IP**: To assign the SNMP Host IP address.

- **UDP Port**: To assign port number. Default: 162
- **Community / Security Name**: The length of "Community / Security Name" string is restricted to 1–32.
- **Security Level**: Indicates what kind of message will send to the Security Level.

  Possible modes are:

  - Info: Send information, warnings, and errors.
  - Warning: Send warnings and errors.
  - Error: Send errors.
- **Security Level**: There are three kinds of choices:
  - NoAuth, NoPriv: No authentication and no privacy.
  - Auth, NoPriv: Authentication and no privacy.
  - Auth, Priv: Authentication and privacy.
- **Authentication Protocol**: Choose MD5 or SHA for authentication.
- **Authentication Password**: The length of "MD5 Authentication Password" is restricted to 8–32
  The length of "SHA Authentication Password" is restricted to 8–40.
- **Privacy Protocol**: You can set DES encryption for UserName.
- **Privacy Password**: The length of "Privacy Password" is restricted to 8–32.

3. Configuration

This chapter describes all the basic network configuration tasks, which include the Ports, Layer 2 network protocol (e.g. VLANs, QoS, IGMP, ACLs and PoE etc.), and any setting of the switch.

3.1 Port

This section describes how to configure the Port detail parameters of the switch, including how to configure, enable, or disable the Port, or to monitor the port's content or status functionality

3.1.1 Configuration

This chapter describes how to view the current port configuration and how to configure ports to non-default settings, including the following:

- Linkup/Linkdown
- Speed (Current and configured)
- Flow Control (Current Rx, Current Tx, and Configured)
- Maximum Frame Size
- Excessive Collision Mode
- Power Control

Web Interface

To configure an Current Port Configuration in the Web interface:

1. Click Configuration, Port, then Configuration
2. Specify the Speed Configured, Flow Control, Maximum Frame size, Excessive Collision mode and Power Control.
3. Click Save.

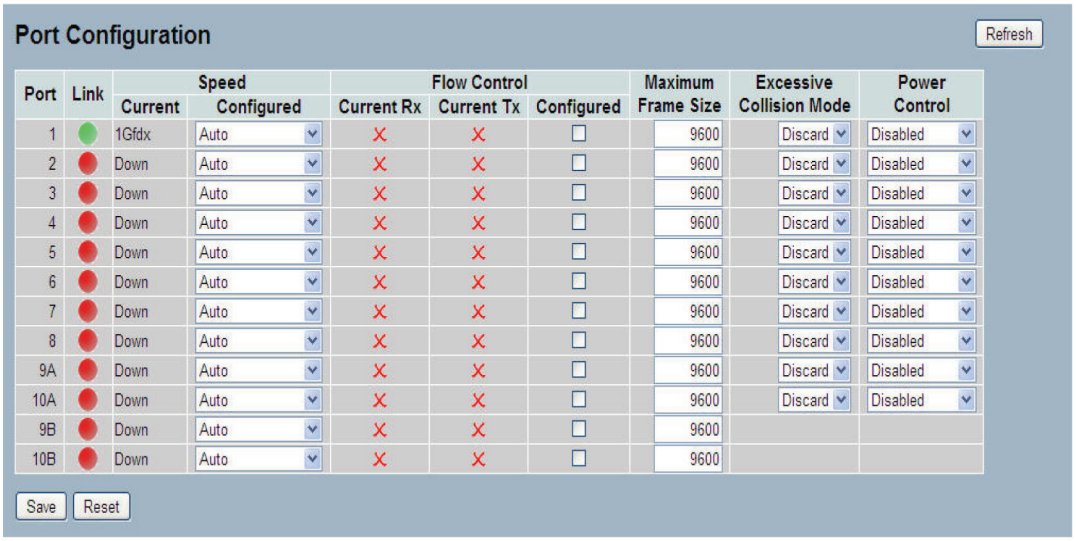


Figure 3-1. The Port Configuration screen.

Parameter Description

- **Port**: This is the logical port number for this row.
- **Link**: The current link state is displayed graphically. Green indicates the link is up and red that it is down.
- **Current Link Speed**: Provides the current link speed of the port.
- **Configured Link Speed**: Select any available link speed for the given switch port.
  - Auto Speed selects the highest speed that is compatible with a link partner.
  - Disabled disables the switch port operation.
- **Flow Control**: When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.

  Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
- **Maximum Frame Size**: Enter the maximum frame size permitted for the switch port, including FCS.
- **Excessive Collision Mode**: Configure port transmit collision behavior.
  - Discard: Discard frame after 16 collisions (default).
  - Restart: Restart backoff algorithm after 16 collisions.
- **Power Control**: The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port.
  - Disabled: All power savings mechanisms disabled.
  - ActiPHY: Link down power savings enabled.
  - PerfectReach: Link up power savings enabled.
  - Enabled: Both link up and link down power savings enabled.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.
- **Icon, upper right of screen (Refresh)**: Click to refresh the Port link Status manually.

3.1.2 Port Description

This section describes how to configure the port's alias and any descriptions for the Port Identity. It prompts the user to create an alphanumeric string describing the full name and version for the system's hardware, software version, and networking application.

Web Interface

To configure an Port Description in the Web interface:

1. Click Configuration, Port, then Port Description.
2. Specify the detail port alias or an alphanumeric string describing the full name and version for the system's hardware, software version, and networking application.
3. Click Save.

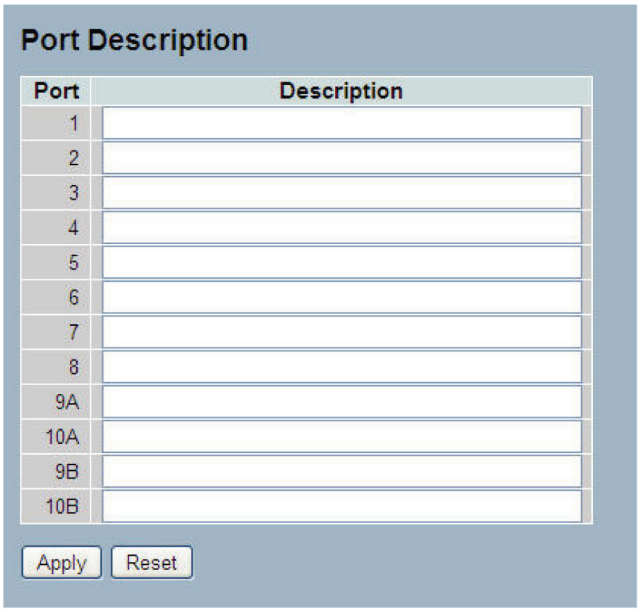


Figure 3-2. The Port Configuration screen.

Parameter Description

- **Port**: This is the logical port number for this row.
- **Description**: Description of device ports cannot include symbols such as " # % & ' + \.
- **Buttons**:
  - Apply: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

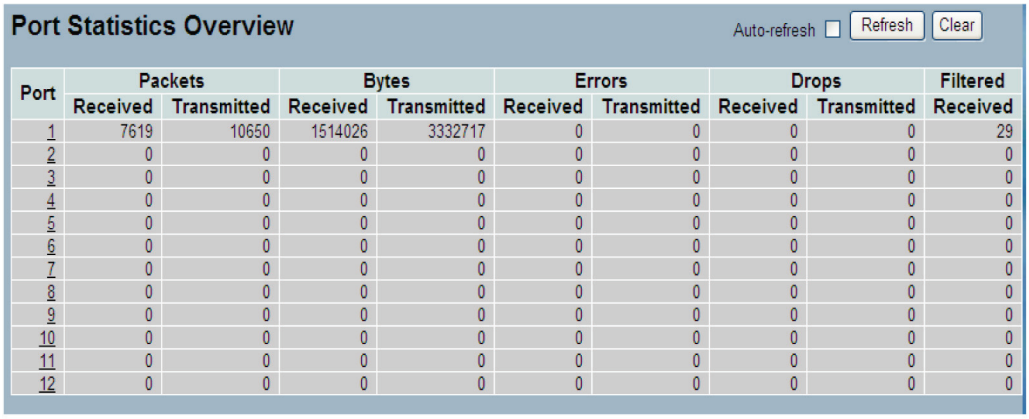
3.1.3 Traffic Overview

This section describes the port statistics information and provides an overview of general traffic statistics for all switch ports.

Web Interface

To Display the Port Statistics Overview in the Web interface:

1. Click Configuration, Port, then Traffic Overview.
2. To set the unit to auto-refresh, check "Auto-refresh".
3. Click "Refresh" to refresh the port statistics or clear all information by clicking "Clear".



Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	7619	10650	1514026	3332717	0	0	0	0	29
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0

Figure 3-3. The Port Statistics Overview screen.

Parameter Description

- **Port**: The logical port for the settings contained in the same row.
- **Packets**: The number of received and transmitted packets per port.
- **Bytes**: The number of received and transmitted bytes per port.
- **Errors**: The number of frames received in error and the number of incomplete transmissions per port.
- **Drops**: The number of frames discarded because of ingress or egress congestion.
- **Filtered**: The number of received frames filtered by the forwarding
- **Auto-refresh**: Check this box if you want the information on this screen to refresh automatically.
- **Icon, upper right of screen (Refresh, Clear)**: Click to refresh or clear the Port Statistics manually.

3.1.4 Detailed Statistics

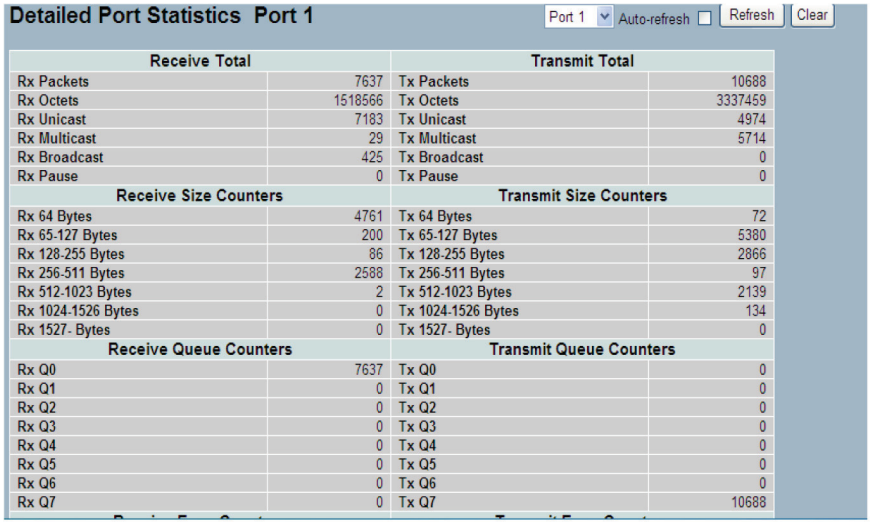
This section describes how to find detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Web Interface

To Display the per port detailed port statistics overview in the Web interface:

1. Click Configuration, Port, then Detailed Port Statistics
2. Scroll the Port Index to select which port you want to show the detailed "Port Statistics overview" .
3. If you want to auto-refresh the information, check the "Auto-refresh" box.
4. Click "Refresh" to refresh the port detailed statistics or clear all information when you click "Clear".



Receive Total		Transmit Total	
Rx Packets	7637	Tx Packets	10688
Rx Octets	1518566	Tx Octets	3337459
Rx Unicast	7183	Tx Unicast	4974
Rx Multicast	29	Tx Multicast	5714
Rx Broadcast	425	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	4761	Tx 64 Bytes	72
Rx 65-127 Bytes	200	Tx 65-127 Bytes	5380
Rx 128-255 Bytes	86	Tx 128-255 Bytes	2866
Rx 256-511 Bytes	2588	Tx 256-511 Bytes	97
Rx 512-1023 Bytes	2	Tx 512-1023 Bytes	2139
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	134
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	7637	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	10688

Figure 3-4. The Port Detail Statistics Overview screen.

Parameter Description

- **Auto-refresh**: Check <Auto-refresh> to refresh the Port Statistics information automatically.
- **Upper left scroll bar**: To scroll which port to display the Port statistics with "Port-0", "Port-1..."

Receive Total and Transmit Total:

- **Rx and Tx Packets**: The number of (good and bad) packets received and transmitted.
- **Rx and Tx Octets**: The number of (good and bad) bytes received and transmitted. Includes FCS, but excludes framing bits.
- **Rx and Tx Unicast**: The number of (good and bad) unicast packets received and transmitted.
- **Rx and Tx Multicast**: The number of (good and bad) multicast packets received and transmitted.
- **Rx and Tx Broadcast**: The number of (good and bad) broadcast packets received and transmitted.
- **Rx and Tx Pause**: A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters: The number of (good and bad) packets split into categories that have been received and transmitted based on their respective frame sizes.

Receive and Transmit Queue Counters: The number of packets per input and output queue received and transmitted.

Receive Queue Counters:

- **Rx Drops**: The number of frames dropped because of lack of receive buffers or egress congestion.
- **Rx CRC/Alignment**: The number of frames received with CRC or alignment errors.
- **Rx Undersize**: The number of short 1 frames received with valid CRC.
- **Rx Oversize**: The number of long 2 frames received with valid CRC.
- **Rx Fragments**: The number of short 1 frames received with invalid CRC.
- **Rx Jabber**: The number of long 2 frames received with invalid CRC.
- **Rx Filtered**: The number of received frames filtered by the forwarding process.
  - Short frames are frames that are smaller than 64 bytes.
  - Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Queue Counters:

- **Tx Drops**: The number of frames dropped because of output buffer congestion.
- **Tx Late/Exc. Coll.**: The number of frames dropped because of excessive or late collisions.
- **Auto-refresh**: Check to refresh the Queuing Counters automatically.
- **Icon, upper right of screen (Refresh, clear)**: Click to refresh the Port Detail Statistics or clear them manually.

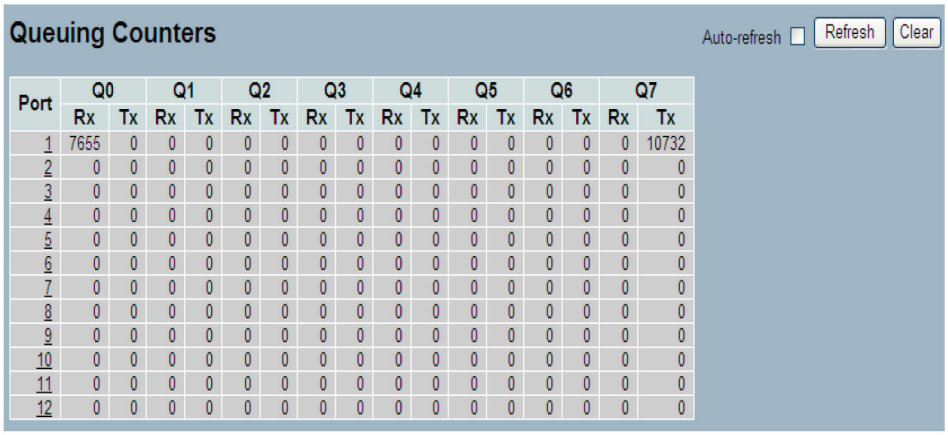
3.1.5 Qos Statistics

This section describes how the switch displays the QoS detailed Queuing Counters for a specific switch port for the different queues for all switch ports.

Web Interface

To Display the Queueing Counters in the Web interface:

1. Click Configuration, Port, then QoS Statistics
2. To auto-refresh the information, check "Auto-refresh".
3. Click "Refresh" to refresh the Queueing Counters or clear all information when you click "Clear".



Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	7655	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10732
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 3-5. Queuing Counters Overview screen.

Parameter Description

- **Port**: The logical port for the settings contained in the same row.
- **Qn**: Qn is the Queue number, QoS queues per port. Q0 is the lowest priority queue.
- **Rx/Tx**: The number of packets received and transmitted per queue.
- **Auto-refresh**: Check <Auto-refresh> to refresh the Queuing Counters automatically.
- **Icons, upper right of screen (Refresh, clear)**: Click to refresh Queuing Counters or clear them manually.

3.1.6 SFP Information

This section describes the SFP module detail information, including connector type, fiber type, wavelength, baud rate, and vendor OUI, etc.

Web Interface

To display the SFP information in the Web interface:

1. Click Configuration, Port, then SFP Information
2. To display the SFP Information.

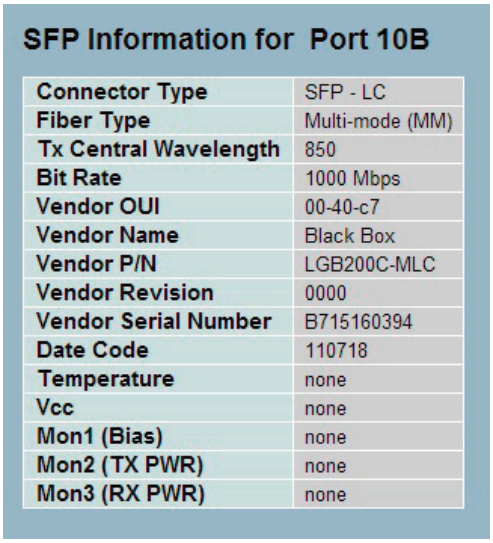


Figure 3-6. The SFP Information Overview screen.

Parameter Description

- **Connector Type**: Displays the connector type: UTP, SC, ST, LC etc.
- **Fiber Type**: Displays the fiber mode, for instance, Multi-Mode, Single-Mode.
- **Tx Central Wavelength**: Displays the fiber optical transmitting central wavelength: 850nm, 1310nm, 1550nm etc.
- **Baud Rate**: Displays the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G etc.
- **Vendor OUI**: Displays the Manufacturer's OUI code, which is assigned by IEEE.
- **Vendor Name**: Displays the company name of the module manufacturer.
- **Vendor P/N**: Displays the product name of the naming by module manufacturer.
- **Vendor Rev (Revision)**: Displays the module revision.
- **Vendor SN (Serial Number)**: Displays the serial number assigned by the manufacturer.
- **Date Code**: Displays the date this SFP module was made.
- **Temperature**: Displays the current temperature of the SFP module.
- **Vcc**: Displays the working DC voltage of the SFP module.
- **Mon1 (Bias) mA**: Displays the bias current of the SFP module.
- **Mon2 (TX PWR)**: Displays the transmit power of the SFP module.
- **Mon3 (RX PWR)**: Displays the receiver power of the SFP module.

3.1.7 EEE

This section enables the user to inspect and configure the current EEE port settings.

EEE is a power saving option that reduces the power usage when there is very low traffic utilization (or no traffic).

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted, all circuits are powered up. The time it takes to power up the circuits is called "wakeup time." The default wake-up time is 17 µs for 1 Gb links and 30 µs for other link speeds. EEE devices must agree upon the value of the wakeup time to make sure that both the receiving device and the transmitting device have all circuits powered up when traffic is transmitted. The devices can exchange information about the devices wakeup time using the LLDP protocol.

For maximizing the power savings, the circuit isn't started at once. Data is made ready, and is queued until 3000 bytes of data are ready to be transmitted. In order not to introduce a large delay in case data less than 3000 bytes needs to be transmitted, data is always transmitted after 48 µs, giving a maximum latency of 48 µs plus the wakeup time.

It is possible to minimize the latency for specific frames by mapping the frames to a specific queue (done with QOS) and then to mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once, and the latency will be reduced to the wakeup time.

Web Interface

To configure the EEE Configuration in the Web interface:

1. Click Configuration, Port, then EEE.
2. Select which port needs the EEE function enabled.
3. The EEE Urgent Queues level ranges from 1 to 8. The queue will postpone the transmsion until 3000 bytes are ready to be transmitted.
4. Click the Save button to save the setting
5. To cancel the setting, click the Reset button to revert to previously saved values.

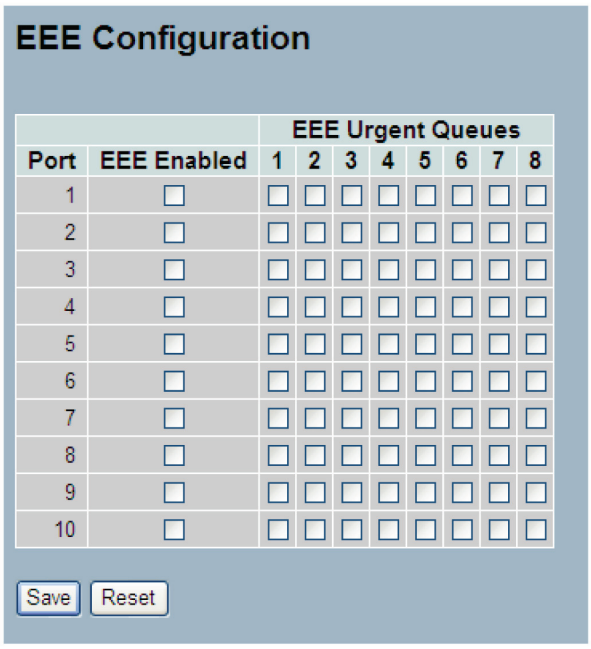


Figure 3-7. The EEE Configuration screen.

Parameter Description

EEE Port Configuration: The EEE port settings relate to the currently selected item, as shown in the page header.

- **Port**: The switch port number of the logical EEE port.
- **EEE Enabled**: Controls whether EEE is enabled for this switch port.
- **EEE Urgent Queues**: Queue sets will activate transmition of frames as soon as any data is available. Otherwise the queue will postpone the transmsion until 3000 bytes are ready to be transmitted.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.2 ACL

The PoE+ Gigabit Managed Switch Eco access control list (ACL) is probably the most commonly used object in the IOS. It is used not only for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into EtherTypes. IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will go over the standard and extended access lists for TCP/IP. To create ACEs for ingress classification, assign a policy for each port. The policy numbers are 1-8, but, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

3.2.1 Ports

This section describes how to configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

Web Interface

To configure the ACL Ports Configuration in the Web interface:

1. Click Configuration, ACL, then Ports.
2. To scroll the specific parameter value to select the correct value for port ACL setting.
3. Click the Save button to save the setting
4. If you want to cancel the setting, click the Reset button. It will revert to previously saved values.
5. After your configuration is complete, you can see the port counter. Click Refresh to update the counter or click Clear to clear any unsaved changes.

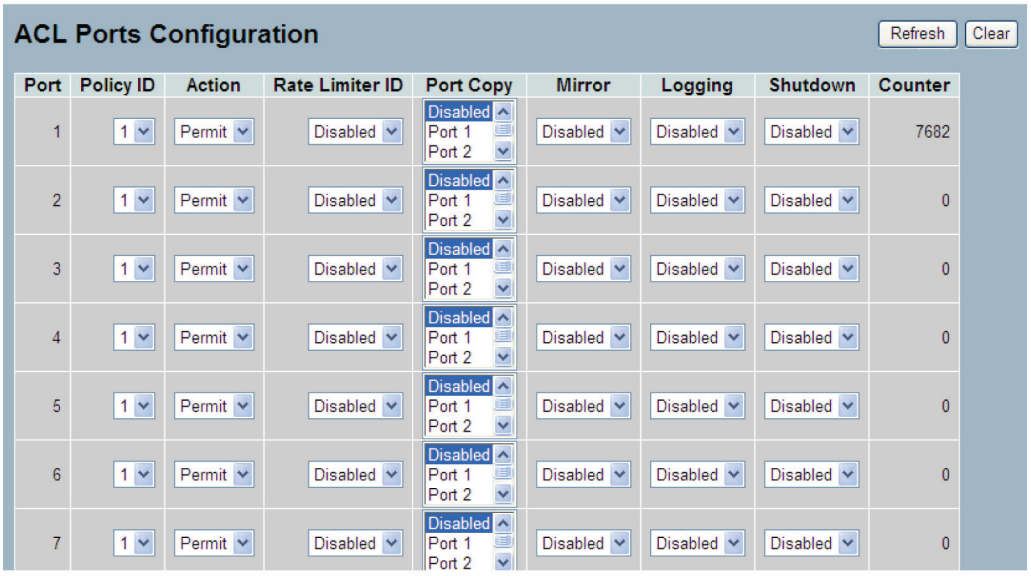


Figure 3-8 The ACL Ports Configuration screen.

Parameter Description

- **Port**: The logical port for the settings contained in the same row.
- **Policy Policy ID**: Select the policy to apply to this port. The values should be 1 through 8. The default value is 1.
- **Action**: Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

- **Rate Limiter ID**: Select which rate limiter to apply on this port. The permitted values are "Disabled" or the values 1 through 16. The default value is "Disabled".
- **Port Copy**: Select which port frames are copied on. The values permitted are "Disabled" or a specific port number. The default value is "Disabled."
- **Mirror**: Specify the mirror operation of this port. The permitted values are:

  - Enabled: Frames received on the port are mirrored.

  - Disabled: Frames received on the port are not mirrored.

  The default value is "Disabled".
- **Logging**: Specify the logging operation of this port. The permitted values are:

  - Enabled: Frames received on the port are stored in the System Log.

  - Disabled: Frames received on the port are not logged.

  The default value is "Disabled". Please note that the System Log memory size and logging rate are limited.
- **Shutdown**: Specify the port shutdown operation of this port. The permitted values are:

  - Enabled: If a frame is received on the port, the port will be disabled.

  - Disabled: Port shutdown is disabled.

  The default value is "Disabled".
- **Counter**: Counts the number of frames that match this ACE.
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.
- **Icons, upper right of screen (Refresh, clear)**: Click to refresh the ACL Ports Configuration or to clear them manually.

3.2.2 Rate Limiters

This section describes how to configure the switch's ACL Rate Limiter parameters. The Rate Limiter Levels from 1 to 16 permit the user to set rate limiter value and units with pps or kbps.

Web Interface

To configure ACL Rate Limiter in the Web interface:

1. Click Configuration, ACL, then Rate Limiter
2. To specific the Rate field and the range from 0 to 3276700.
3. To scroll the Unit with pps or kbps
4. Click the Save button to save the setting
5. If you want to cancel a setting, click the Reset button to revert to previously saved values.

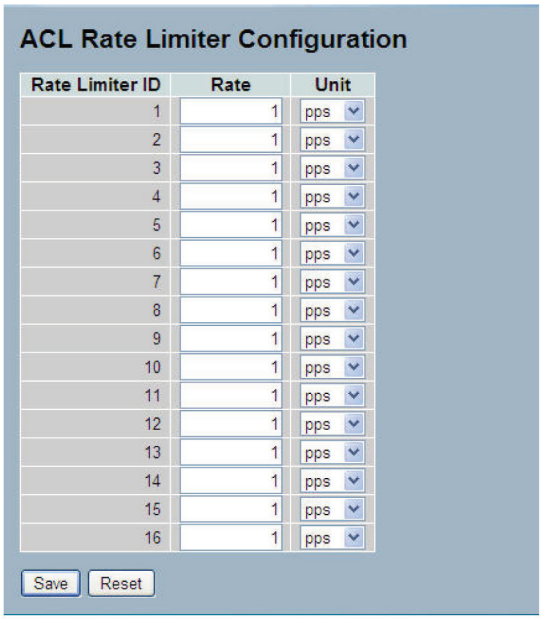


Figure 3-9. The ACL Rate Limiter Configuration screen.

Parameter Description

- **Rate Limiter ID**: The rate limiter ID for the settings contained in the same row.
- **Rate**: Permitted values are: 0–3,276,700 in pps or 0, 100, 200, 300, ..., 1,000,000 in kbps.
- **Unit**: Specify the rate unit. Values permitted are: pps (packets per second) and kbps (kilobits per second).
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.2.3 Access Control List

This section describes how to configure Access Control List rule. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed an the priority is highest.

Web Interface

To configure Access Control List in the Web interface:

1. Click Configuration, ACL, then Configuration.
2. Click the button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list).
3. To specific the parameter of the ACE.
4. Click the Save button to save the setting.
5. To cancel a setting, click the Reset button. It will revert to previously saved values.
6. When editing an entry on the Access Control Entry (ACE) Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Then specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).

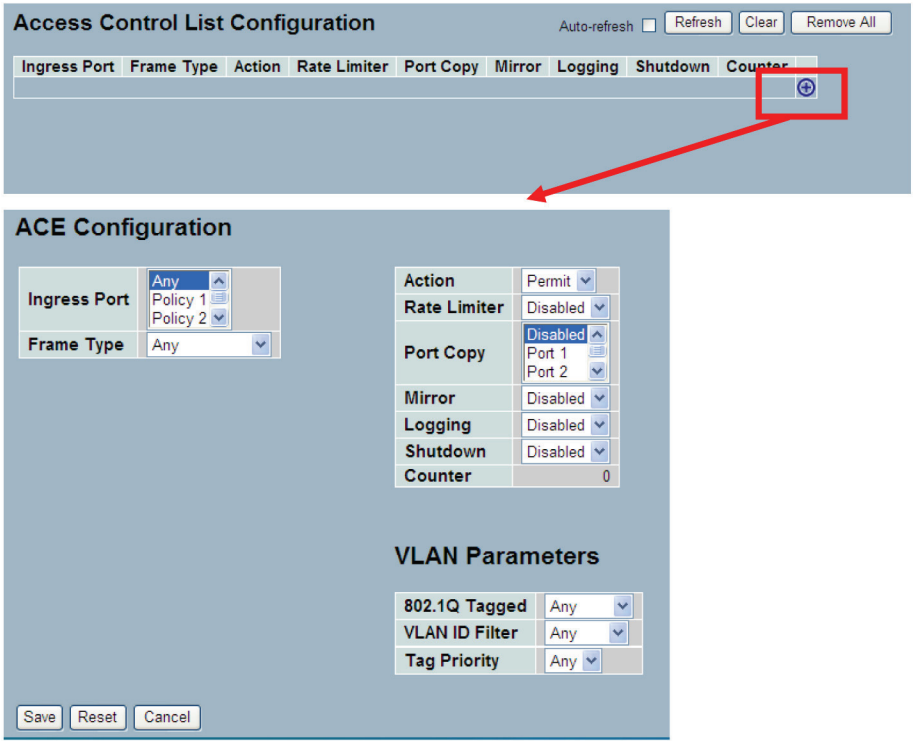


Figure 3-10. The ACL Rate Limiter Configuration screen.

Parameter Description

- **Ingress Port** : Indicates the ingress port of the ACE. Possible values are:
  - Any: The ACE will match any ingress port.
  - Policy: The ACE will match ingress ports with a specific policy.
  - Port: The ACE will match a specific ingress port.
- **Frame Type**: Indicates the frame type of the ACE. Possible values are:
  - Any: The ACE will match any frame type.
  - Ethernet Type: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
  - ARP: The ACE will match ARP/RARP frames.
  - IPv4: The ACE will match all IPv4 frames.
- **Action**: Indicates the forwarding action of the ACE.
  - Permit: Frames matching the ACE may be forwarded and learned.
  - Deny: Frames matching the ACE are dropped.
- **Rate Limiter**: Indicates the rate limiter number of the ACE. The permitted range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
- **Port Copy**: Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The permitted values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.
- **Mirror**: Specify the mirror operation of this port. The permitted values are:
  - Enabled: Frames received on the port are mirrored.
  - Disabled: Frames received on the port are not mirrored. The default value is "Disabled".
- **Logging**: Indicates the logging operation of the ACE. Possible values are:
  - Enabled: Frames matching the ACE are stored in the System Log.
  - Disabled: Frames matching the ACE are not logged.

  Please note that the System Log memory size and logging rate is limited.
- **Shutdown**: Indicates the port shutdown operation of the ACE. Possible values are:

- Enabled: If a frame matches the ACE, the ingress port will be disabled.
- Disabled: Port shutdown is disabled for the ACE.

- **Counter**: The counter indicates the number of times the ACE was hit by a frame.

Modification Buttons: You can modify each ACE in the table using the following buttons:

: Inserts a new ACE before the current row.

: Edits the ACE row.

: Moves the ACE up the list.

: Moves the ACE down the list.

: Deletes the ACE.

: The lowest plus sign adds a new entry at the bottom of the ACE listings.

- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.
  - Cancel: Click to cancel changes.
- **Auto-refresh**: Click to refresh the information automatically.
- **Icons, upper right of screen (Refresh, Clear, Remove All)**: Click to refresh the ACL Configuration. Click Clear to reset changes manually. Click Remove All to clean up all ACL configurations on the table.

3.2.4 ACL Status

This section describes how to show the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware because of hardware limitations. The maximum number of ACEs is 256 on each switch.

Web Interface

To display the ACL status in the Web interface:

1. Click Configuration, ACL, then ACL status
2. To set the switch to auto-refresh the information, click "Auto-refresh".
3. Click "Refresh" to refresh the ACL Status.

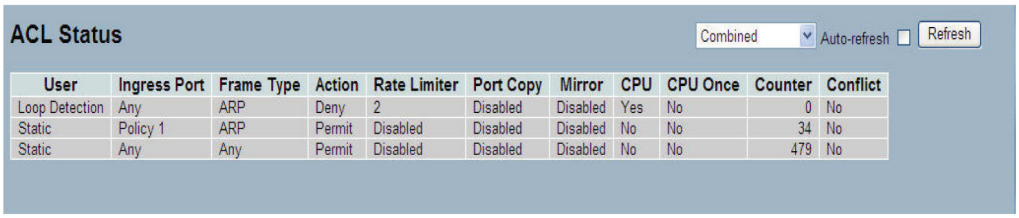


Figure 3-11. The ACL Rate Limiter Configuration screen.

Parameter Description

- **User**: Indicates the ACL user.
- **Ingress Port**: Indicates the ingress port of the ACE. Possible values are:
  - Any: The ACE will match any ingress port.
  - Policy: The ACE will match ingress ports with a specific policy.
  - Port: The ACE will match a specific ingress port.
- **Frame Type**: Indicates the frame type of the ACE. Possible values are:
  - Any: The ACE will match any frame type.
  - EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
  - ARP: The ACE will match ARP/RARP frames.
  - IPv4: The ACE will match all IPv4 frames.
- **Action**: Indicates the forwarding action of the ACE.

- Permit: Frames matching the ACE may be forwarded and learned.
- Deny: Frames matching the ACE are dropped.

- **Rate Limiter**: Indicates the rate limiter number of the ACE. The range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
- **Port Copy**: Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The permitted values are disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.
- **Mirror**: Specify the mirror operation of this port. The permitted values are:
  - Enabled: Frames received on the port are mirrored.
  - Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

- **CPU**: Forward packet that matched the specific ACE to CPU.
- **CPU Once**: Forward first packet that matched the specific ACE to CPU.
- **Counter**: The counter indicates the number of times the ACE was hit by a frame.
- **Conflict**: Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware because of hardware limitations.
- **Auto-refresh**: Click auto-refresh to refresh the information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the ACL status information manually.

3.3 Aggregation

The Aggregation is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full-duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can use your current Ethernet equipment to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port.

3.3.1 Static Trunk

Ports using Static Trunk as their trunk method can choose their unique Static GroupID to form a logic "trunked port". The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregated together to form a "logic trunked port". Black Box strongly recommends using Static Trunk on both ends of a link.

NOTE: Low speed links will stay in a "not ready" state when using static trunk to aggregate with high speed links.

Web Interface

To configure the Trunk Aggregation Hash mode and Aggregation Group in the Web interface:

1. Click Configuration, Static Trunk, and then Aggregation Mode Configuration.
2. Click "Evoke Aggregation Group ID and Port members" to enable or disable the aggregation mode function.
3. Click the Save button to save the setting
4. To cancel the setting, click the Reset button to revert to previously saved values.

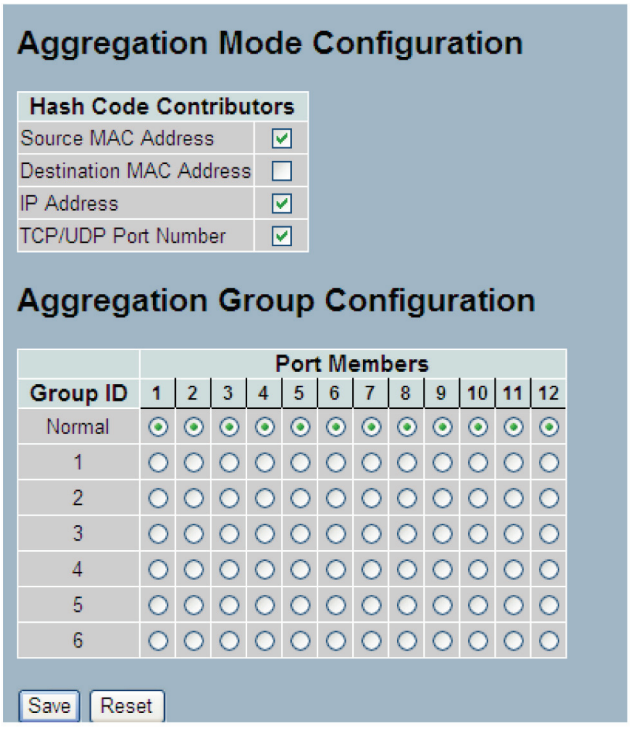


Figure 3-12. The Aggregation Mode Configuration screen.

Parameter Description

Hash Code Contributors

- Source MAC Address: The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address or uncheck to disable. By default, Source MAC Address is enabled.
- Destination MAC Address: The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
- IP Address: The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
- TCP/UDP Port Number: The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Aggregation Group Configuration

- Locality: Indicates the aggregation group type. This field is only valid for switches.
  - Global: The group members may reside on different units. The device supports two 8-port global aggregations.
  - Local: The group members reside on the same unit. Each local aggregation may consist of up to 16 members.
- Group ID: Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
- Port Members: Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
- Buttons:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.3.2 LACP

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID to form a logic "trunked port". The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a "trunk group" (also called aggregator).

LACP is safer than the other trunking method, static trunk.

Configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them as well. An LACP trunk group with more than one ready member-ports is a "real trunked" group. An LACP trunk group with only one or less than one ready member-ports is not a "real trunked" group.

Web Interface

To configure the Trunk Aggregation LACP parameters in the Web interface:

1. Click Configuration, LACP, Configuration.
2. Select enable or disable the LACP on the port of the switch. Select the Key parameter with Auto or Specific (Default is Auto).
3. Select the Role from the Active or Passive pulldown menu. (Default is Active).
4. Click the Save Button to save the setting.
5. To cancel the setting, click the Reset button to revert to previously saved values.

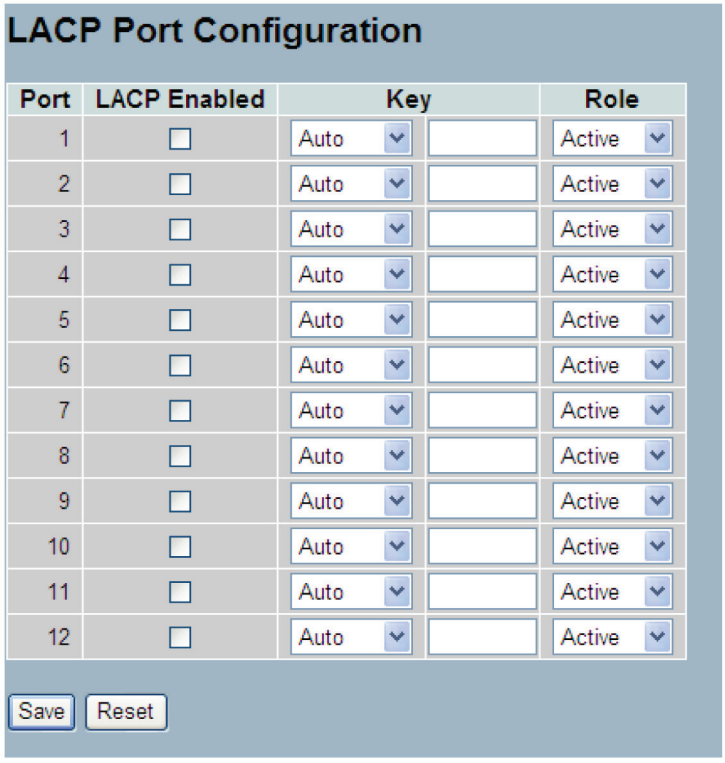


Figure 3-13. The LACP Port Configuration screen.

Parameter Description

- **Port**: The switch port number.
- **LACP Enabled**: Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form a maximum of 12 LLAGs per switch and 2 GLAGs.

- **Key**: The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
- **Role**: The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

System Status

When you set the LACP function on the switch, it provides a status overview for all LACP instances

Web Interface

To display the LACP System status in the Web interface:

1. Click Configuration, LACP, System Status
2. To set the switch to auto-refresh the information, check "Auto-refresh".
3. Click " Refresh" to refresh the LACP System Status.

Figure 3-14. The LACP System Status screen

Parameter Description

- **Aggr ID**: The Aggregation ID associated with this aggregation instance. For LLAG the ID is shown as 'isid:aggr-id' and for GLAGs as "aggr-id".
- **Partner System ID**: The system ID (MAC address) of the aggregation partner.
- **Partner Key**: The key that the partner has assigned to this aggregation ID.
- **Last Changed**: The time since this aggregation changed.
- **Local Ports**: Shows which ports are a part of this aggregation for this switch. The format is: "Switch ID:Port."
- **Auto-refresh**: Click auto-refresh to refresh the information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the LACP System status information manually.

Port Status

When you set the LACP function on the switch, a Port Status overview for all LACP instances is enabled.

Web Interface

To display the LACP Port Status in the Web interface:

1. Click Configuration, LACP, Port Status
2. To set the switch to auto-refresh the information, check "Auto-refresh".
3. Click "Refresh" to refresh the LACP Port Status.

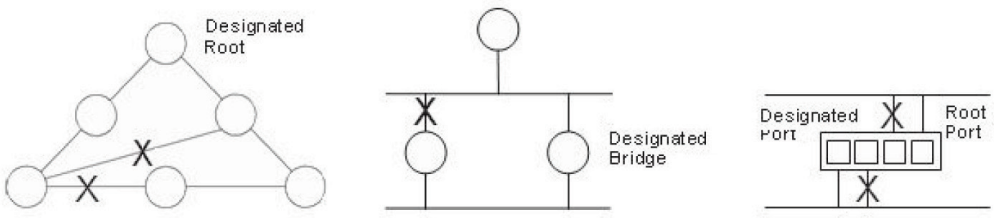


Figure 3-15. The LACP Status screen.

Parameter Description

- **Port**: The switch port number.
- **LACP**: "Yes" means that LACP is enabled and the port link is up. "No" means that LACP is not enabled or that the port link is down. "Backup" means that the port could not join the aggregation group but will join if other port leaves. Meanwhile its LACP status is disabled.
- **Key**: The key assigned to this port. Only ports with the same key can aggregate together.
- **Aggr ID**: The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.
- **Partner System ID**: The partner's System ID (MAC address).
- **Partner Port**: The partner's port number connected to this port.
- **Auto-refresh**: Click auto-refresh to refresh the information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the LACP port status information manually.

Port Statistics

When you complete the LACP function on the switch, a Port Statistics overview for all LACP instances is enabled.

Web Interface

To display the LACP Port status in the Web interface:

2. To set the switch to auto-refresh the information, check "Auto-refresh".

3. Click "Refresh" to refresh the LACP Port Statistics.

Figure 3-16. The LACP Statistics screen.

Parameter Description

- **Port**: The switch port number.
- **LACP Received**: The number of LACP frames that have been received at each port.
- **LACP Transmitted**: The number of LACP frames that have been sent from each port.
- **Discarded**: The number of unknown or illegal LACP frames that have been discarded at each port.
- **Auto-refresh**: Click auto-refresh to refresh the information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the LACP port statistics information manually.

3.4 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges, or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge, or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP uses a distributed algorithm to select a bridging device (an STP- compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

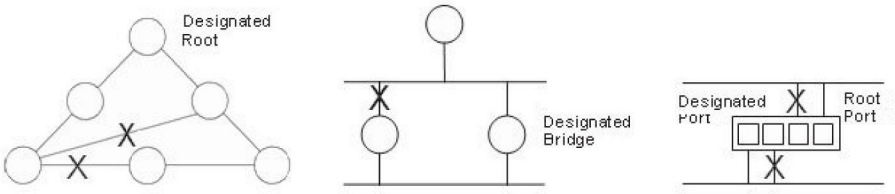


Figure 3-17. The Spanning Tree protocol.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

3.4.1 Bridge Settings

This section describes how to configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings that are used by all STP Bridge instances in the swtich.

Web Interface

To configure the Spanning Tree Bridge Settings parameters in the Web interface:

1. Click Configuration, Spanning Tree, Bridge Settings.
2. Scoll to select your parameters and the values in Basic Settings.
3. Scoll to select your parameters and the values in Advanced Settings
4. Click save to save the settings.
5. To cancel the settings changes, click the Reset button to revert to previously saved values.

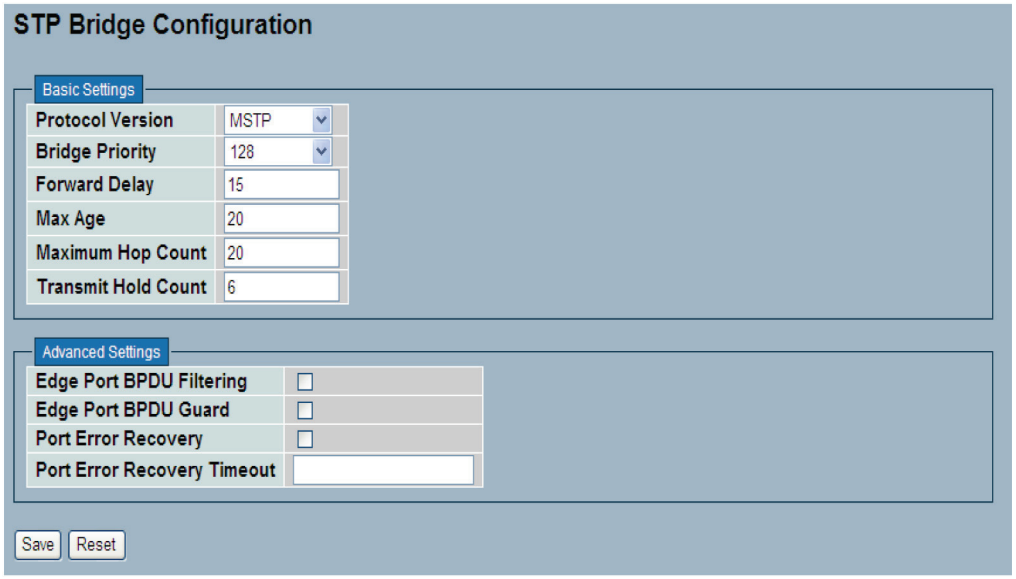


Figure 3-18. The STP Bridge Configuration screen.

Parameter Description

Basic Settings

- **Protocol Version**: The STP protocol version setting. Valid values are STP, RSTP, and MSTP.
- **Bridge Priority**: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
- **Forward Delay**: The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
- **Max Age**: The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.
- **Maximum Hop Count**: Defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region, or how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.
- **Transmit Hold Count**: The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDUs per second.

Advanced Settings

- **Edge Port BPDU Filtering**: Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
- **Edge Port BPDU Guard**: Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
- **Port Error Recovery**: Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
- **Port Error Recovery Timeout**: The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.4.2. MSTI Mapping

When you implement a Spanning Tree protocol on the switch, the CIST is not available for explicit mapping, because it receives the VLANs that are not explicitly mapped. For this reason, you need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with a comma and/or a space. A VLAN can only be mapped to one MSTI. An unused MSTI should simply be left empty, (i.e. with no VLANs mapped to it.)

This section describes it allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree MSTI Mapping parameters in the Web interface:

1. Click Configuration, Spanning Tree, MSTI Mapping.
2. Specify the configuration identification parameters in the field. Specify the VLANs Mapped blank field.
3. Click the Save button to save the setting.
4. To cancel the setting, click the Reset button to revert to previously saved values.

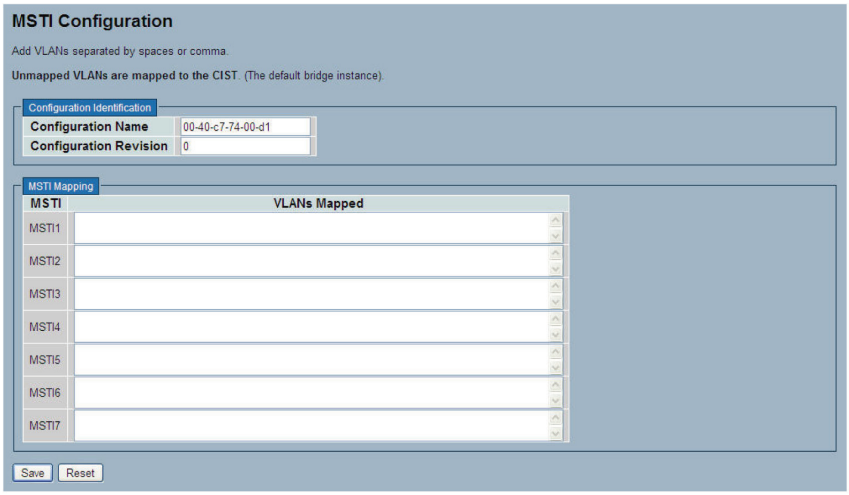


Figure 3-19. The MSTI Configuration screen.

Parameter Description

Configuration Identification

- **Configuration Name**: The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration to share spanning trees for MSTI's (Intra-region). The name should not exceed 32 characters.
- **Configuration Revision**: The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

- **MSTI**: The bridge instance. The CIST is not available for explicit mapping, because it receives the VLANs not explicitly mapped.
- **VLANs Mapped**: The list of VLANs mapped to the MSTI. The VLANs must be separated with a comma and/or a space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs).
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.4.3 MSTI Priorities

When you implement a Spanning Tree protocol on the switch, that is a bridge instance. The CIST is the default instance, and it is always active because it controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier.

This section describes it and enables the user to inspect and change the STP MSTI bridge instance priority configurations.

Web Interface

To configure the Spanning Tree MSTI Priorities parameters in the Web interface:

1. Click Configuration, Spanning Tree, MSTI Priorities.
2. Scroll the Priority maximum is 240. Default is 128.
3. Click the Save button to save the setting.
4. To cancel the settings changes, click the Reset button to revert to previously saved values.

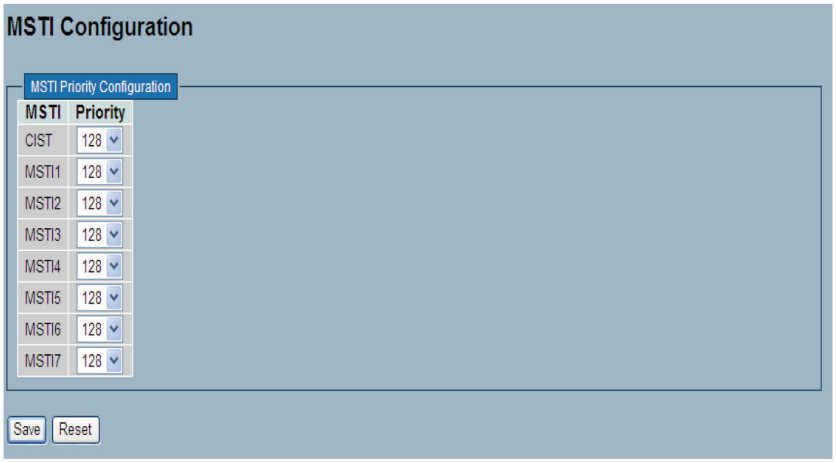


Figure 3-20. The MSTI Configuration screen.

Parameter Description

- MSTI: The bridge instance. The CIST is the default instance, always active.
- Priority: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.
- Buttons:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.4.4 CIST Ports

When you implement a Spanning Tree protocol on the switch, that is a bridge instance. You need to configure the CIST Ports. This section describes how it enables the user to inspect the current STP CIST port configurations and change them if needed.

Web Interface

To configure the Spanning Tree CIST Ports parameters in the Web interface:

1. Click Configuration, Spanning Tree, CIST Ports.
2. Scroll and evoke to set all parameters of CIST Aggregated Port Configuration.
3. Evoke to enable or disable the STP, then scoll and evoke to set all parameters of the CIST normal Port configuration.
4. Click the Save button to save the setting.
5. To cancel the setting, click the Reset button to revert to previously saved values.

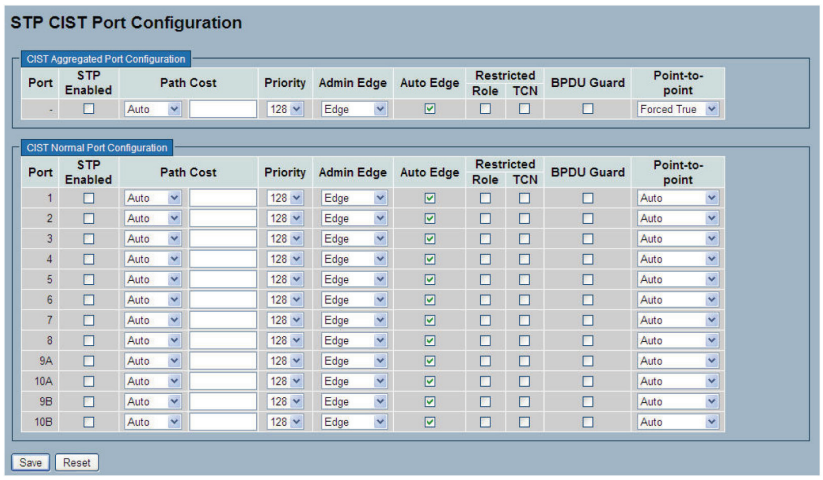


Figure 3-21. The STP CIST Port Configuration screen.

Parameter Description

- **Port**: The switch port number of the logical STP port.
- **STP Enabled**: Controls whether STP is enabled on this switch port.
- **Path Cost**: Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

- **Priority**: Controls the port priority. This can be used to control priority of ports having identical port cost. (See 3.4.3 MSTI Priorities).
- **operEdge (state flag)**: This is the operational flag describing whether the port is connecting directly to edgedevices. (No Bridges attached.) Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.
- **AdminEdge**: This controls whether the operEdge flag should start as set or cleared (the initial operEdge state when a port is initialized).
- **AutoEdge**: This setting controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDUs are received on the port or not.
- **Restricted Role**: If enabled, this setting causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
- **Restricted TCN**: If enabled, this setting causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
- **BPDU Guard**: If enabled, this setting causes the port to disable itself upon receiving valid BPDUs. Contrary to the similar bridge setting, the port edge status does not affect this setting. A port entering error-disabled state because of this setting is subject to the bridge Port Error Recovery setting as well.
- **Point to Point**: Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.4.5 MSTI Ports

This section enables the user to inspect or adjust the current STP MSTI port configuration. An MSTI port is a virtual port, which is represented separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. It contains MSTI port settings for physical and aggregated ports.

Web Interface

To configure the Spanning Tree MSTI Port Configuration parameters in the Web interface:

1. Click Configuration, Spanning Tree, MSTI Ports.
2. Scroll to select the MST1 or other MSTI Port.
3. Click Get to set the detail parameters of the MSTI Ports.
4. Scroll to set all parameters of the MSTI Port configuration.
5. Click the Save button to save the setting.
6. To cancel the setting, click the Reset button to revert to previously saved values.

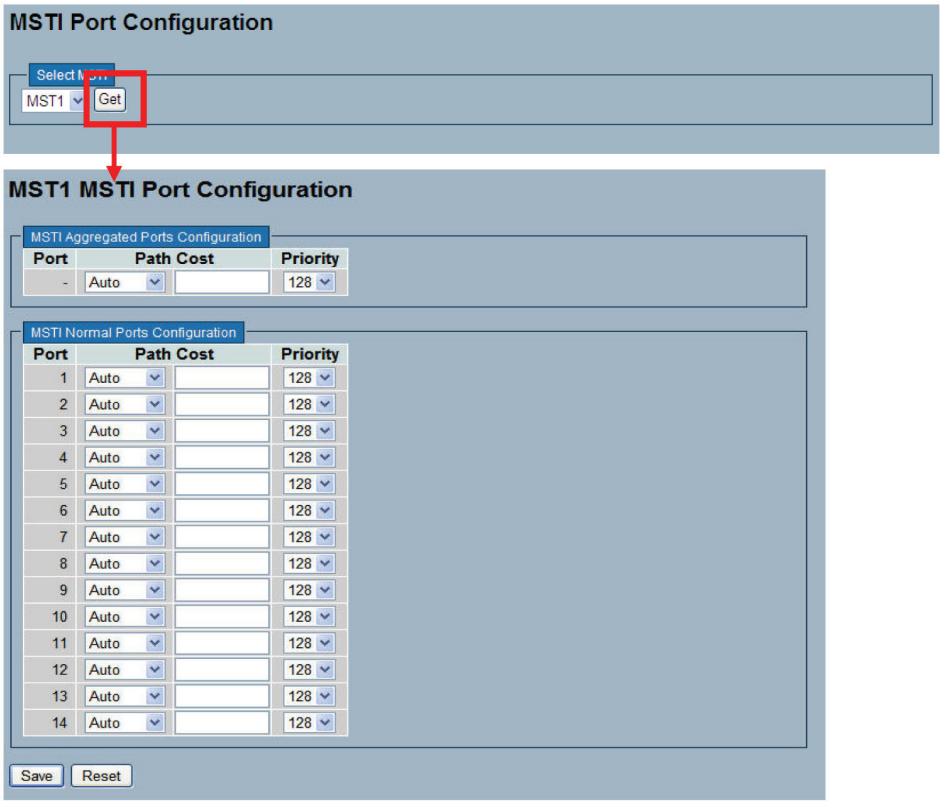


Figure 3-22. The MSTI Port Configuration screen.

Parameter Description

- **Port**: The switch port number of the corresponding STP CIST (and MSTI) port.
- **Path Cost**: Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

- **Priority**: Controls the port priority. This can be used to control priority of ports having identical port cost. (See 3.4.3 MSTI Priorities).
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.4.6 Bridge Status

After you complete the MSTI Port configuration, confibure the Bridge Status. This section provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the following information:

Web Interface

To display the STP Bridges status in the Web interface:

1. Click Configuration, Spanning Tree, STP Bridges
2. To auto-refresh the information, check "Auto-refresh".
3. Click "Refresh" to refresh the STP Bridges.

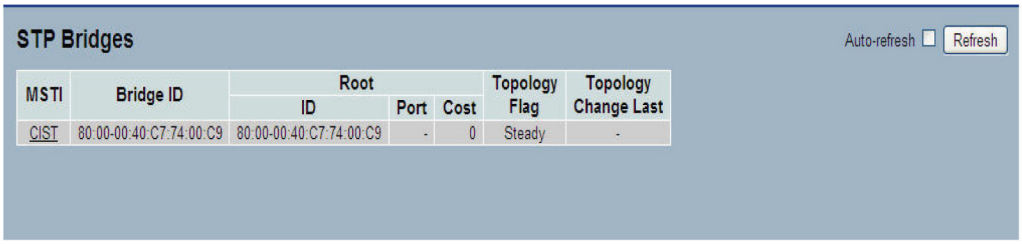


Figure 3-23. The STP Bridge Status screen.

Parameter Description

- **MSTI**: The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
- **Bridge ID**: The Bridge ID of this Bridge instance.
- **Root ID**: The Bridge ID of the currently elected root bridge.
- **Root Port**: The switch port currently assigned the root port role.
- **Root Cost**: Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
- **Topology Flag**: The current state of the Topology Change Flag of this Bridge instance.
- **Topology Change Last**: The time since last Topology Change occurred.
- **Auto-refresh**: Check Auto-refresh to refresh the information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the STP Bridges status information manually.

3.4.7 Port Status

After you complete the STP configuration, configure the switch display for the STP Port Status. This section enables you to display the STP CIST port status for physical ports of the currently selected switch.

Web Interface

To display the STP Port status in the Web interface:

1. Click Configuration, Spanning Tree, STP Port Status.
2. To auto-refresh the information, check "Auto-refresh".
3. Click "Refresh" to refresh the STP Bridges.

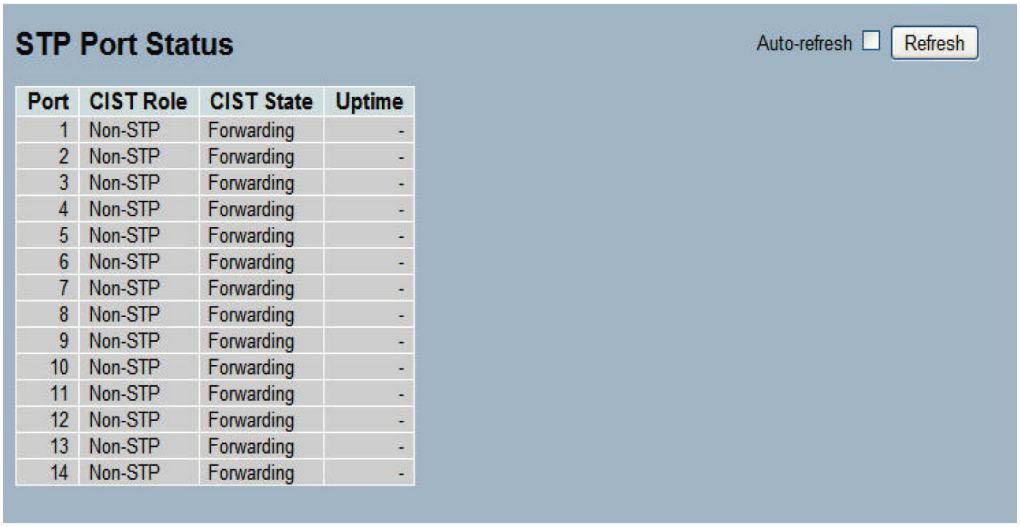


Figure 3-24. The STP Port Status screen.

Parameter Description

- **Port**: The switch port number of the logical STP port.
- **CIST Role**: The current STP port role of the CIST port. The port role can be one of the following values:

  - AlternatePort, Backup Port, RootPort, DesignatedPort Disabled.

- **CIST State**: The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding.
- **Uptime**: The time since the bridge port was last initialized.
- **Auto-refresh**: Check "Auto-refresh" to refresh the information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the STP Port status information manually.

3.4.8 Port Statistics

After you complete the STP configuration, configure the switch to display the STP Statistics. This section enables you to adjust the STP Statistics detail counters of bridge ports in the currently selected switch.

Web Interface

To display the STP Port status in the Web interface:

1. Click Configuration, Spanning Tree, Port Statistics
2. To auto-refresh the information, check "Auto-refresh".
3. Click "Refresh" to refresh the STP Bridges.

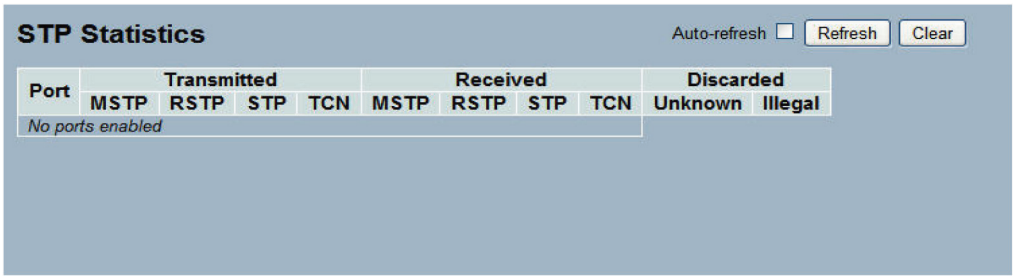


Figure 3-25. The STP Statistics screen.

Parameter Description

- **Port**: The switch port number of the logical STP port.
- **MSTP**: The number of MSTP Configuration BPDUs received/transmitted on the port.
- **RSTP**: The number of RSTP Configuration BPDUs received/transmitted on the port.
- **STP**: The number of legacy STP Configuration BPDUs received/transmitted on the port.
- **TCN**: The number of (legacy) Topology Change Notification BPDUs received/transmitted on the port.
- **Discarded Unknown**: The number of unknown Spanning Tree BPDUs received (and discarded) on the port.
- **Discarded Illegal**: The number of illegal Spanning Tree BPDUs received (and discarded) on the port.
- **Auto-refresh**: Check Auto-refresh to refresh the information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the STP Statistics information manually.

3.5 Loop Detection

Loop detection is used to detect the presence of traffic. When a switch receives a packet's (looping detection frame) MAC address that's the same as the MAC address from the port, loop detection occurs. The port will be locked when it receives the looping detection frames. To restore the locked port, delete the looping path, then click on "Resume."

Configuration

The section describes how to set Loop Detection.

Web Interface

To configure the Loop detection parameters in the Web interface:

1. Click Configuration, Loop detection, Configuration.
2. Enable or disable the port loop detection.
3. Click on the Save button to save the setting.
4. To cancel the setting, click the Reset button. The loop detection parameters will revert to their previously saved values.

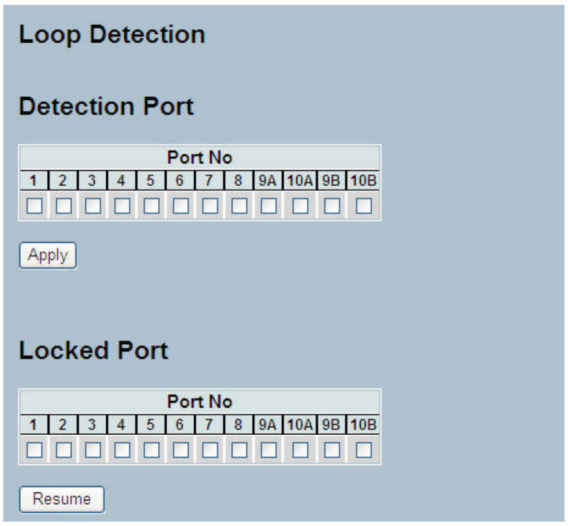


Figure 3-26. Loop Detection Configuration screen.

Parameter description:

- **Port No:** Display the port number (1–10).
- **Detection Port - Enable:** When you select a port and enable that port's loop detection, the port can detect loops. If it detects a loop, the port will be locked. If it does not detect a loop, the port remains unlocked.
- **Locked Port - Resume:** To unlock the port, choose Resume.

3.6 IGMP Snooping

This function is used to establish the multicast groups to forward the multicast packet to the member ports, and, in doing so, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as broadcast packets. Without IGMP Snooping, the multicast packet forwarding function is plain, and nothing is different from broadcast packet.

A switch-supported IGMP Snooping, with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

3.6.1 Basic Configuration

This section describes how to set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

Web Interface

To configure the IGMP Snooping parameters in the Web interface:

1. Click Configuration, IGMP Snooping, Basic Configuration.
2. Check to select which Global configuration to enable or disable.
3. Check which port wants to become a Router Port or enable/disable the Fast Leave function.
4. Scroll to set the Throttling parameter.
5. Click the Save button to save the setting.
6. To cancel your changes, click the Reset button to revert to previously saved values.

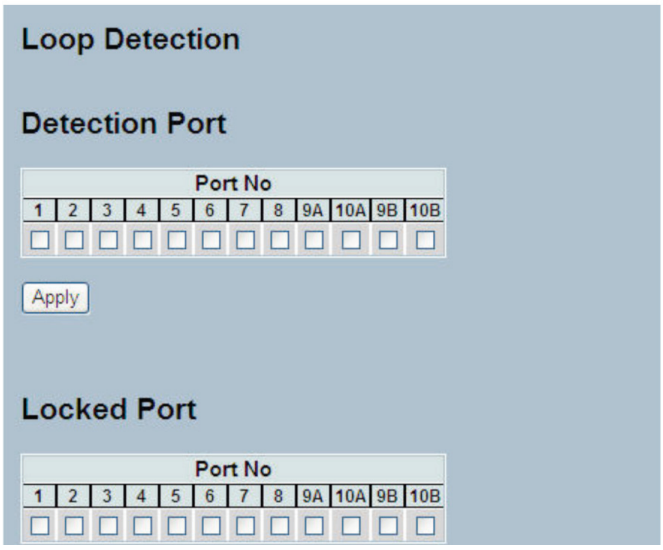


Figure 3-27. The IGMP Snooping Configuration screen.

Parameter Description

- **Snooping Enabled**: Enable the Global IGMP Snooping.
- **Unregistered IPMCv4 Flooding Enabled**: Enable unregistered IPMCv4 traffic flooding.
- **IGMP SSM Range**: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range. Format: (IP address/sub mask).
- **Proxy Enabled**: Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
- **Port**: Shows the physical port index of switch.
- **Router Port**: Specifies which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
- **Fast Leave**: Enable the fast leave on the port.
- **Throttling**: Enable to limit the number of multicast groups to which a switch port can belong.
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.6.2 VLAN Configuration

This section describes the VLAN configuration setting process, integrated with IGMP Snooping function. Each setting page shows up to 99 entries from the VLAN table, (the default is 20), selected through the "entries per page" input field. When first visited, the Web page will show the first 20 entries from the beginning of the VLAN Table. The first entry that is displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the next closest VLAN Table match.

Web Interface

To configure the IGMP Snooping VLAN Configuration in the Web interface:

1. Click Configuration, IGMP Snooping, VLAN Configuration.
2. Click to select enable or disable Snooping, IGMP Querier. Specify the parameters in the blank field.
3. Click the Refresh button to update the data or click << or >> to display previous entry or next entry.
4. Click the Save button to save the setting
5. Click the Reset button to undo any changes made locally and revert to previously saved values.

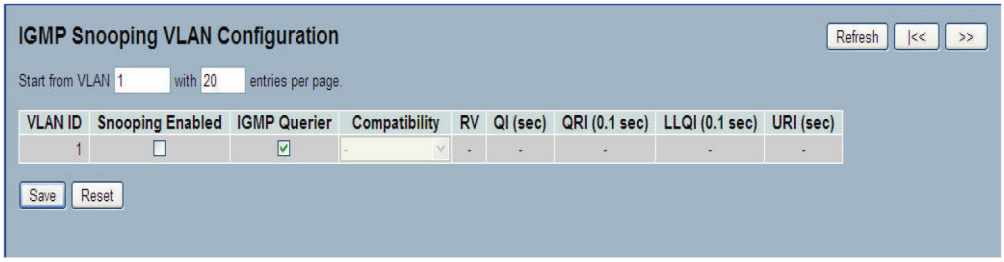


Figure 3-28. The IGMP Snooping VLAN Configuration screen.

Parameter Description

- **VLAN ID**: It displays the VLAN ID of the entry.
- **Snooping Enabled**: Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected.
- **IGMP Querier**: Sends IGMP Query messages onto a particular link. Enable the IGMP Querier in the VLAN.
- **Compatibility**: Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The range of selections includes IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3. The default compatibility value is IGMP-Auto.
- **RV**: Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The permitted range is 1 to 255; the default Robustness Variable value is 2.
- **QI**: The Query Interval is the interval between General Queries sent by the Querier. The permitted range is 1 to 31744 seconds; the default Query Interval is 125 seconds.
- **QRI**: Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The range of values is 0 to 31744 in tenths of seconds; the default query response interval is 100 in tenths of seconds (10 seconds).
- **LLQI (LMQI for IGMP)**: Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The permitted range is 0 to 31744 in tenths of seconds; the default LMQI is 10 in tenths of seconds (1 second).
- **URI**: Unsolicited Report Interval. This is the time between repetitions of a host's initial report of membership in a group. The range of values is 0 to 31744 seconds, and the default unsolicited report interval is 1 second.
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

- **Icons, upper right of screen (Refresh, |<<, >>)**: Click to refresh the displayed table starting from the "VLAN" input fields. Or click "|<<" to update the table starting from the first entry in the VLAN table, i.e. the entry with the lowest VLAN ID. For other entries click ">> " to update the table, starting with the entry after the last entry currently displayed.

3.6.3 Port Group Filtering

This section describes how to set the IGMP Port Group Filtering. In some network application environments, such as metropolitan or multiple-dwelling unit (MDU) installations, a user might want to control the multicast groups to which a user on a switch port can belong. This feature allows the user to control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

Web Interface

To configure the IGMP Snooping Port Group Configuration in the Web interface:

1. Click Configuration, IGMP Snooping, Port Group Filtering
2. Click Add new Filtering Group
3. Scroll the Port to enable the Port Group Filtering. Specify the Filtering Groups in the blank field.
4. Click the Save button to save the setting.
5. To cancel the setting, click the Reset button to revert to previously saved values.

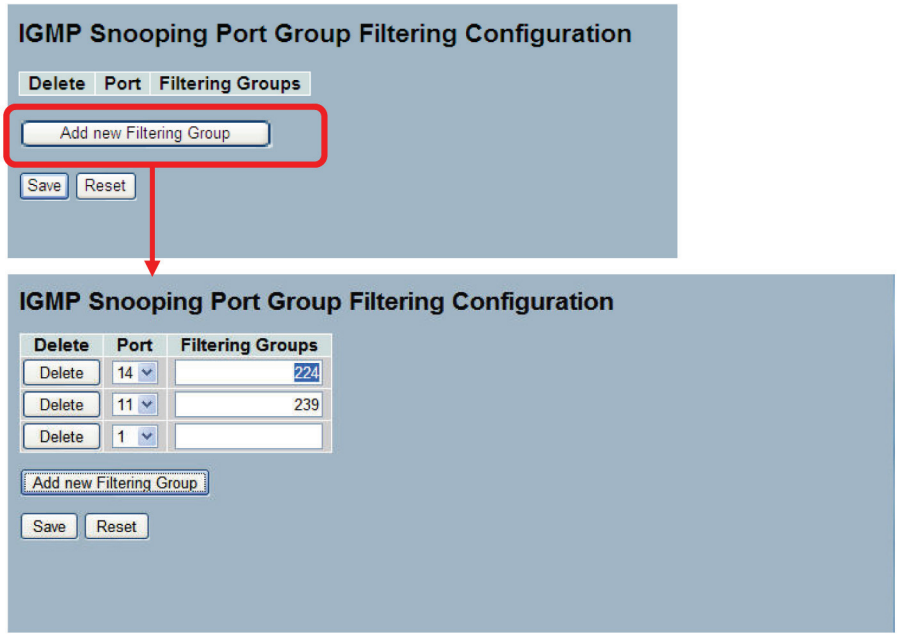


Figure 3-29. The IGMP Snooping Port Group Filtering Configuration screen.

Parameter Description

- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **Port**: To evoke the port, enable the IGMP Snooping Port Group Filtering function.
- **Filtering Groups**: The IP Multicast Group that will be filtered.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.6.4 Status

After completing the IGMP Snooping configuration, the switch will display the IGMP Snooping Status. This section enables you to view the IGMP Snooping detail status.

Web Interface

To display the IGMP Snooping status in the Web interface:

1. Click Configuration, IGMP Snooping, Status.
2. If you want to auto-refresh the information, check "Auto-refresh".
3. Click "Refresh" to refresh the IGMP Snooping Status.
4. Click "Clear" to clear the IGMP Snooping Status.

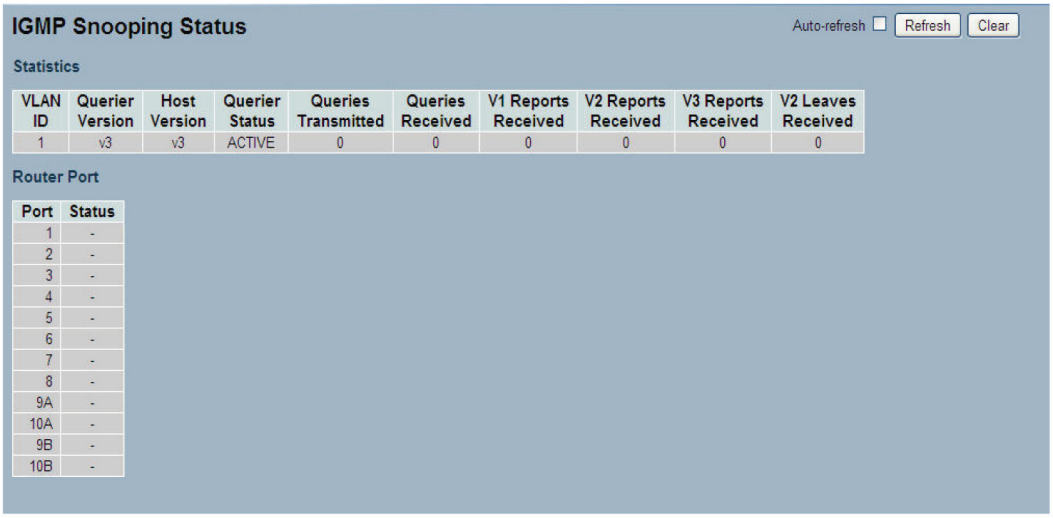


Figure 3-30. The IGMP Snooping Status screen.

Parameter Description

- **VLAN ID**: The VLAN ID of the entry.
- **Querier Version**: The current working Querier Version.
- **Host Version**: the current working Host Version.
- **Querier Status**: Shows the Querier status is "Active" or "Idle".
- **Queries Transmitted**: The number of Queries transmitted.
- **Queries Received**: The number of Queries received.
- **V1 Reports Received**: The number of V1 Reports received.
- **V2 Reports Received**: The number of V2 Reports received.
- **V3 Reports Received**: The number of V3 Reports received.
- **V2 Leaves Received**: The number of V2 Leaves received.
- **Auto-refresh**: Check "Auto-refresh" to set the switch to refresh the log automatically.
- **Icons, upper right of screen (Refresh, clear)**: Click to refresh the Status or clear it manually.

3.6.5 Group Information

After setting the IGMP Snooping function, you can view the IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. It will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

Web Interface

To display the IGMP Snooping Group Information in the Web interface:

1. Click Configuration, IGMP Snooping, Group Information
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click " Refresh" to refresh a entry of the IGMP Snooping Groups Information.
4. Click "<< or >>" to move to previous or next entry.

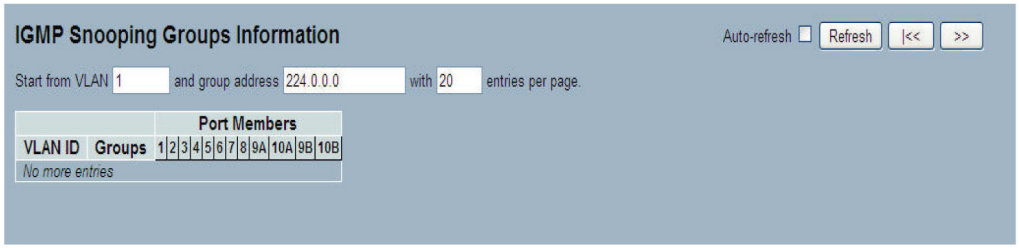


Figure 3-31. The IGMP Snooping Groups Information screen.

Parameter Description

Navigating the IGMP Group Table: The "Start from VLAN" and "Group" input fields allow the user to select the starting point in the IGMP Group Table. The system will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in he displayed table.

IGMP Group Table Columns

- **VLAN ID**: VLAN ID of the group.
- **Groups**: Group address of the group displayed.
- **Port Members**: Ports under this group.
- **Auto-refresh**: Check "Auto-refresh" to enable the device to refresh the log automatically.
- **Icons, upper right of screen (Refresh, <<, >>)**: Click these icons to refresh the IGMP Group Status, to navigate to the next/up page or to the next entry.

3.6.6 IPv4 SSM information

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S, G). By subscribing to this channel, the receiver host is indicating that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

Addresses in the range 232.0.0.0/8 (232.0.0.0 to 232.255.255.255) are reserved for SSM by IANA. In the switch, you can configure SSM for arbitrary IP multicast addresses also.

Web Interface

To display the IGMPv3 IPv4 SSM Information in the Web interface:

1. Click Configuration, IGMP Snooping, IPv4 SSM Information
2. To set the information here to auto-refresh, check the “Auto-refresh” box.
3. Click “Refresh” to refresh the information manually.
4. Click “<< or >>” to navigate to previous or next entry.

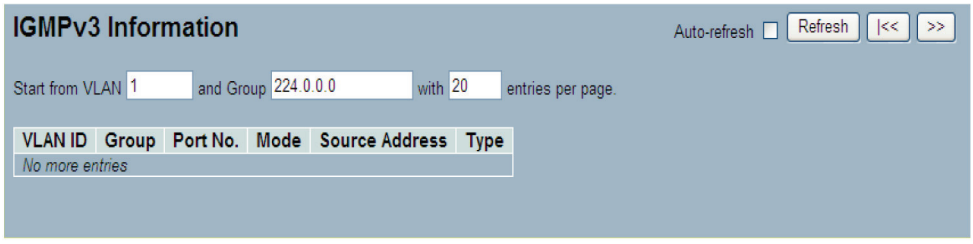


Figure 3-32. The IGMP IPv4 SSM Information screen.

Parameter Description

Navigating the IGMPv3 Information Table

Each page shows up to 99 entries from the IGMPv3 SSM (Source Specific Multicast) Information table, default being 20, selected through the “entries per page” input field. When first visited, the Web page will show the first 20 entries from the beginning of the IGMPv3 Information Table.

The “Start from VLAN”, and “group” input fields allow the user to select the starting point in the IGMPv3 Information Table. Clicking the button will update the displayed table starting from that or the closest next IGMPv3 Information Table match. In addition, the two input fields will, with a button click, assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the Refresh button to start over.

- **VLAN ID**: The VLAN ID of the group.
- **Group**: The Group address of the group displayed.
- **Port**: The switch port number.

- **Mode**: Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
- **Source Address**: The IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to 128.
- **Type**: Indicates the Type. It can be either Allow or Deny.
- **Auto-refresh**: To set the unit to auto-refresh the information, check the "auto-refresh" box.
- **Icons, upper right of screen (Refresh, <<, >>)**: Click Refresh to refresh the IGMP Group Status manually. Click the arrows to navigate to the next page or entry.

3.7 MLD Snooping

Curiously enough, a network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn't interact with it. (Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.)

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts.

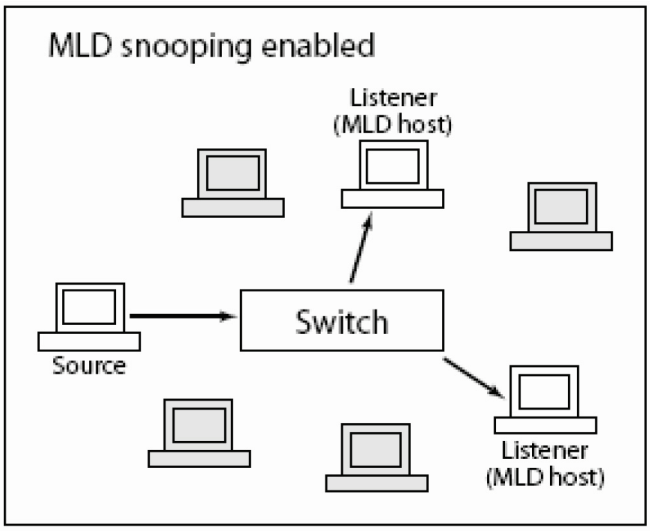


Figure 3-33. MLD Snooping Enabled screen.

3.7.1 Basic Configuration

This section will show you how to configure the MLD Snooping basic configuration and parameters:

Web Interface:

To configure the MLD Snooping Configuration in the Web interface:

1. Click Configuration, MLD Snooping, Basic Configuration.
2. Check to enable or disable the Global configuration parameters. Check the port to join Router port and Fast Leave.
3. Scroll to select the Throttling mode with unlimited or 1 to 10.
4. Click to save the setting.
5. To cancel the setting, click the Reset button to revert to previously saved values.

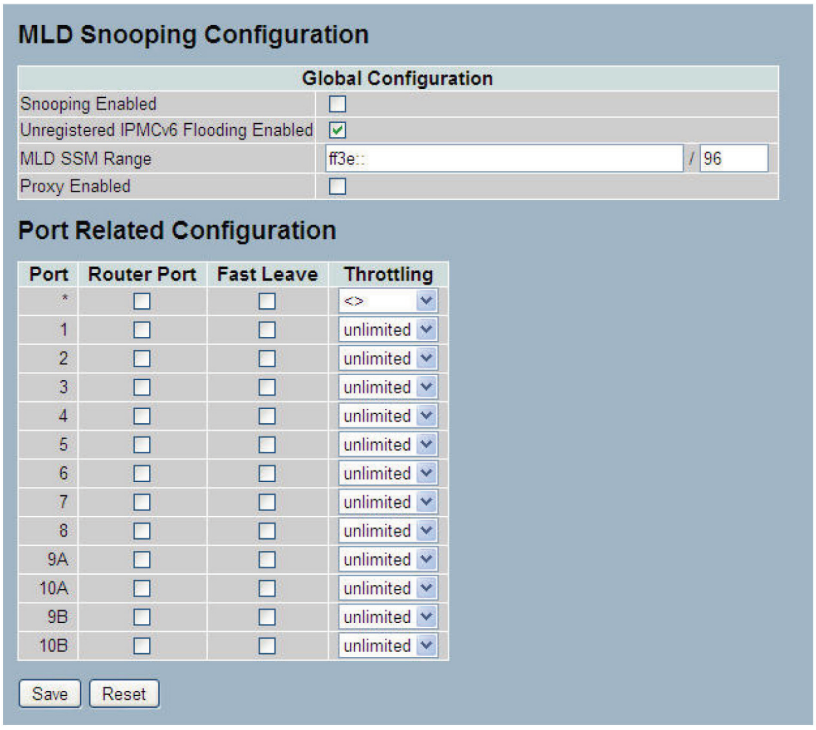


Figure 3-34. The MLD Snooping Basic Configuration screen.

Parameter Description

- **Snooping Enabled**: Enables the Global MLD Snooping.
- **Unregistered IPMCv6 Flooding Enabled**: Enable unregistered IPMCv6 traffic flooding. Please note that disabling unregistered IPMCv6 traffic flooding may lead to failure of Neighbor Discovery.
- **MLD SSM Range**: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (Using IPv6 Address) range.
- **Proxy Enabled**: Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
- **Port**: The Port index what you enable or disable the MLD Snooping function.
- **Router Port**: Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
- **Fast Leave**: To evoke to enable the fast leave on the port.
- **Throttling**: Enable to limit the number of multicast groups to which a switch port can belong.
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.7.2 VLAN Configuration

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts. The switch will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached, the text "No more entries" is shown in the displayed table. Use the Refresh button to start over.

Web Interface

To configure the MLD Snooping VLAN Configuration in the Web interface:

1. Click Configuration, MLD Snooping, VLAN Configuration.
2. Specify the VLAN ID with the number of entries per page.
3. Click "Refresh" to refresh an entry.
4. Click "<< or >>" to move to the previous or next entry.

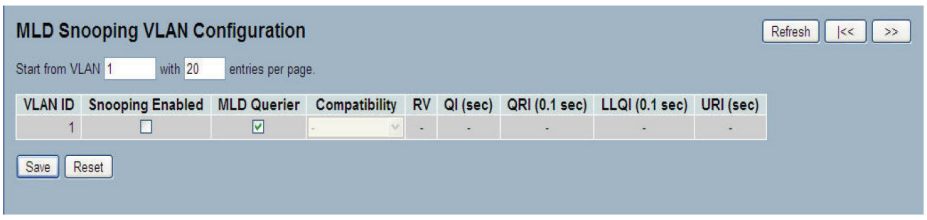


Figure 3-35. The MLD Snooping VLAN Configuration screen.

Parameter Description

- **VLAN ID**: The VLAN ID of the entry.
- **Snooping Enabled**: Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected.
- **MLD Querier**: A router sends MLD Query messages to a particular link. This Router is called the Querier. Enable the MLD Querier in the VLAN.
- **Compatibility**: Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. Possible selections include: MLD-Auto, Forced MLDv1, and Forced MLDv2. The default compatibility value is MLD-Auto.
- **RV**: Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The range is 1 to 255; the default robustness variable value is 2.
- **QI**: Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The range is 1 to 31744 seconds; the default query interval is 125 seconds.
- **QRI**: Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The range is 0 to 31744 in tenths of seconds; the default query response interval is 100 in tenths of seconds (10 seconds).
- **LLQI (LMQI for IGMP)**: Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The range is 0 to 31744 in tenths of seconds, the default last listener query interval is 10 in tenths of seconds (one second).
- **URI**: Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

- **Icons, upper right of screen (Refresh, <<, >>)**: Click "Refresh" to refresh the IGMP Group Status manually; click the arrows to navigaate to the next page or entry.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.7.3 Port Group Filtering

This section describes how to set Port Group Filtering for the MLD Snooping function to add new groups and safety policies.

Web Interface

To configure the MLD Snooping Port Group Configuration in the Web interface:

1. Click Configuration, MLD Snooping, Port Group Filtering Configuration.
2. Click the Add new Filtering Group.
3. Specify the Filtering Groups with entries per page.
4. Click the Save button to save the setting.
5. To cancel your changes, click the Reset button to revert to previously saved values.

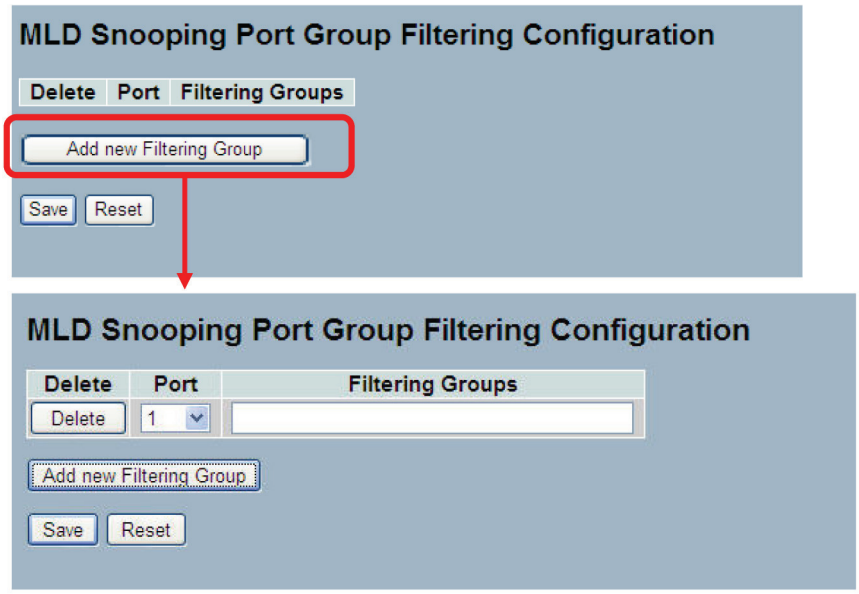


Figure 3-36. The MLD Snooping Port Group Filtering Configuration screen.

Parameter Description

- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **Port**: The logical port for the settings. You can evoke to enable the port to join filtering group.
- **Filtering Groups**: The IP Multicast Group that will be filtered.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.7.4 Status

This section describes how to display the MLD Snooping Status.

Web Interface

To display the MLD Snooping Status in the Web interface:

1. Click Configuration, MLD Snooping, Status
2. If you want to auto-refresh the information, check “Auto-refresh”
3. Click “Refresh” to refresh the MLD Snooping Status information.
4. Click “Clear” to clear the MLD Snooping Status window.

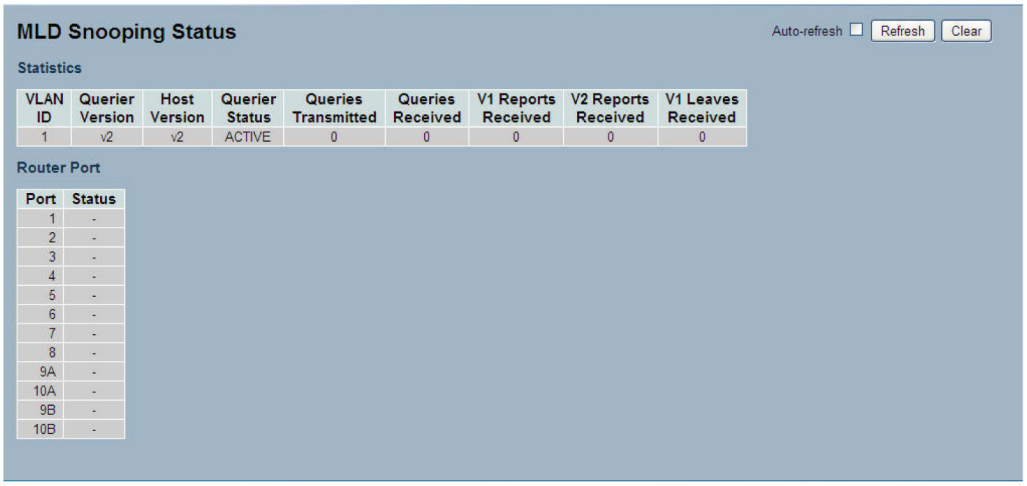


Figure 3-37. The MLD Snooping Status screen.

Parameter Description

- **VLAN ID**: The VLAN ID of the entry.
- **Querier Version**: The current working Querier Version.
- **Host Version**: The current working Host Version.
- **Querier Status**: Shows whether the Querier status is “ACTIVE” or “IDLE”.
- **Queries Transmitted**: The number of Queries transmitted.
- **Queries Received**: The number of Queries received.
- **V1 Reports Received**: The number of V1 Reports received.
- **V2 Reports Received**: The number of V2 Reports received.
- **V1 Leaves Received**: The number of V1 Leaves received.
- **Auto-refresh**: To set the unit to auto-refresh the information, check the “auto-refresh” box.
- **Icons, upper right of screen (Refresh, <<, >>)**: Click Refresh to refresh the MLD Group Status manually. Click the arrows to navigate to the next page or entry.

3.7.5 Group Information

This section describes how to set MLD Snooping Groups Information. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table.

Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the Web page will show the first 20 entries from the beginning of the MLD Group Table.

Web Interface

To display the MLD Snooping Group information in the Web interface:

1. Click Configuration, MLD Snooping, Group Information.
2. To auto-refresh the information, check "Auto-refresh".
3. Click "Refresh" to refresh the MLD Snooping Group Information.
4. Click "Clear" to clear the MLD Snooping Groups information.

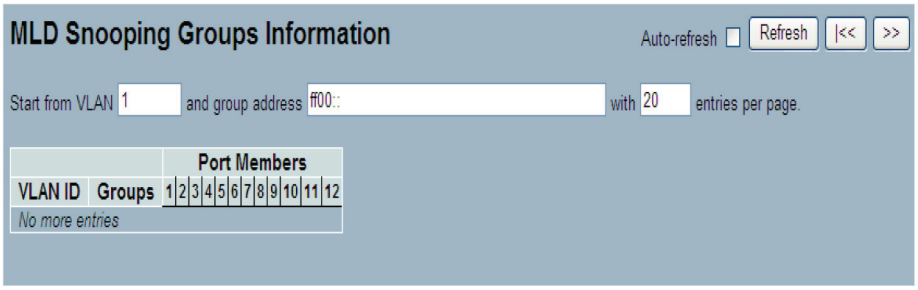


Figure 3-38. The MLD Snooping Groups Information screen.

Parameter Description

Navigating the MLD Group Table

Each page shows up to 99 entries from the MLD Group table, with the default being 20, selected through the "entries per page" input field. When first visited, the Web page will show the first 20 entries from the beginning of the MLD Group Table. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Click the button to update the displayed table, starting from the group address indicated or the next closest address.

MLD Group Table Match

In addition, the two input fields will, with the click of a button, assume the value of the first displayed entry, allowing for continuous refresh with the same start address. It will use the last entry displayed as a basis for the next lookup. When the end is reached, the text "No more entries" will be shown in the displayed table. Use the Refresh button to start over.

MLD Snooping Information Table Columns

- **VLAN ID**: VLAN ID of the group.
- **Groups**: Group address of the group displayed.
- **Port Members**: Ports under this group.
- **Auto-refresh**: To set the unit to auto-refresh the information, check the "auto-refresh" box.
- **Icons, upper right of screen (Refresh, <<, >>)**: Click Refresh to refresh the MLD Snooping Groups Status manually. Click the arrows to navigate to the next page or entry.

3.7.6 IPv6 SSM Information

This section describes how to configure the entries in the MLDv2 Information Table. The MLDv2 Information Table is sorted first by VLAN ID, then by group, and then by Port No. Different source addresses belonging to the same group are treated as a single entry.

Each page shows up to 64 entries from the MLDv2 SSM (Source Specific Multicast) Information table, the default being 20, selected through the "entries per page" input field. When first visited, the form will show the first 20 entries from the beginning of the MLDv2 Information Table. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLDv2 Information Table.

Web Interface

To display the MLDv2 IPv6 SSM Information in the Web interface:

1. Click Configuration, MLD Snooping, IPv6 SSM Information.
2. To auto-refresh the information, click Auto-refresh.
3. Click "Refresh" to refresh a particular entry.
4. Click "<< or >> " to move to previous or next entry.

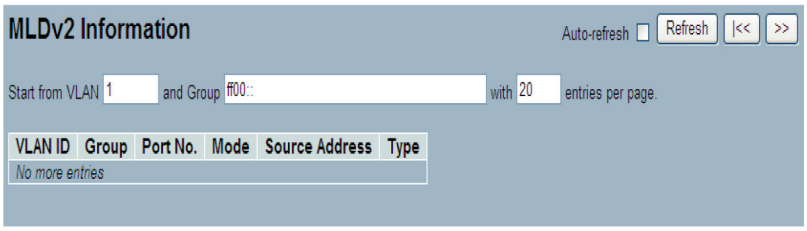


Figure 3-39. The MLDv2 Information screen.

Parameter Description

- **VLAN ID**: VLAN ID of the group.
- **Group**: The Group address of the group displayed.
- **Port No.**: Switch port number.
- **Mode**: The filtering mode maintained on a (VLAN ID, port number, or Group Address) basis. It can be either Include or Exclude.
- **Source Address**: IP Address of the source. The system limits the total number of IP source addresses for filtering to 128.
- **Type**: Indicates the Type. It can be either Allow or Deny.

3.8 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

3.8.1 Configuration

This section describes how to set the MVR basic Configuration and other parameters in the switch.

Web Interface

To configure the MLD Snooping Port Group Configuration in the Web interface:

1. Click Configuration, MVR, Configuration.
2. Scroll to the MVR mode to enable or disable and Scroll to Set All Parameters.
3. Click the Save button to save the setting.
4. To cancel, click the Reset button to revert to previously saved values

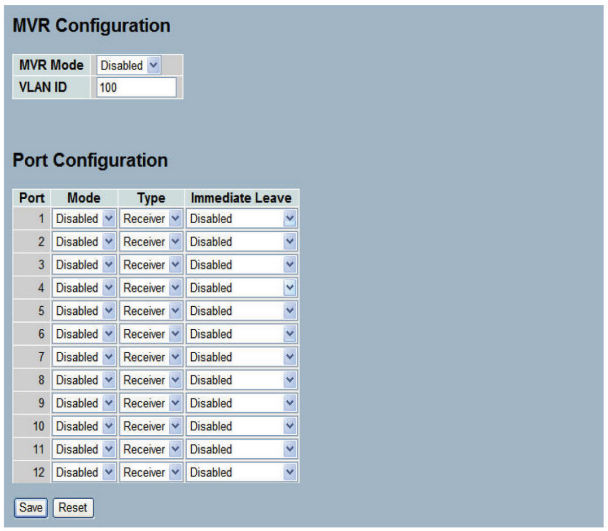


Figure 3-40. The MVR Configuration screen.

Parameter Description

- **MVR Mode**: Enable/Disable the Global MVR.
- **VLAN ID**: Specify the Multicast VLAN ID.
- **Mode**: Enable MVR on the port.
- **Type**: Specify the MVR port type on the port.
- **Immediate Leave**: Enable the fast leave on the port.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.8.2 Groups Information

This section describes how to display the MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group.

Web Interface

To display the MVR Groups Information in the Web interface:

1. Click Configuration, MVR, Groups Information.
2. To set the unit to auto-refresh the information, check the "Auto-refresh" box.
3. Click "Refresh" to refresh the information.
4. Click "<< or >> " to move to previous or next entry.

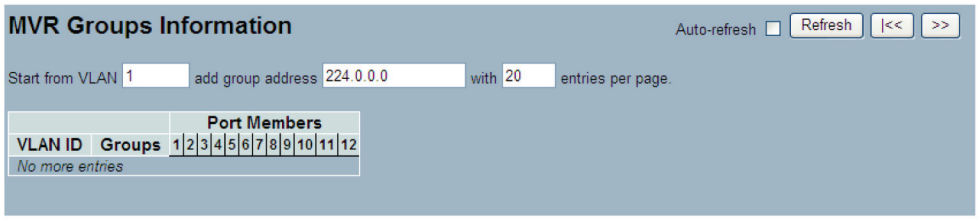


Figure 3-41: MVR Groups Information screen.

Parameter Description

MVR Group Table Columns

- **VLAN ID**: VLAN ID of the group.
- **Groups**: Group ID of the group displayed.
- **Port Members**: Ports under this group.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icons, upper right of screen (Refresh, <<, >>)**: Click them to refresh the MVR Group information manually; click the arrows to navigate to the next page or entry.

3.8.3 Statistics

This section describes the switch will display the MVR detail statistics after you had configured MVR on the switch. It provides the detail MVR statistics information.

Web Interface

To display the MVR statistics information in the Web interface:

1. Click Configuration, MVR, Statistics.
2. To set the unit to auto-refresh the information, check the "Auto-refresh" box.
3. Click "Refresh" to refresh the information.
4. Click "<< or >> " to move to previous or next entry.

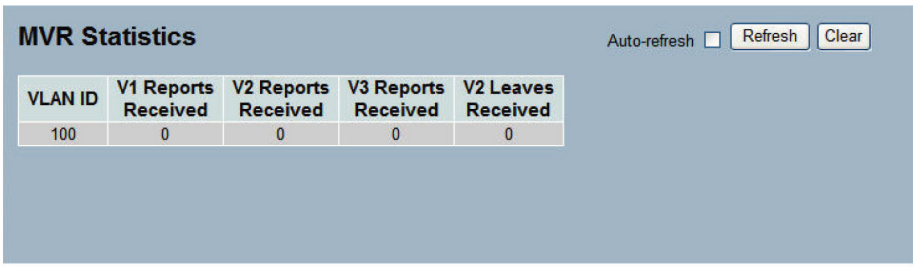


Figure 3-42: MVR Statistics information screen.

Parameter Description

- **VLAN ID**: The Multicast VLAN ID.
- **V1 Reports Received**: The number of V1 Reports received.
- **V2 Reports Received**: The number of V2 Reports received.
- **V3 Reports Received**: The number of V3 Reports received.
- **V2 Leaves Received**: The number of V2 Leaves received.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icons, upper right of screen (Refresh, <<, >>)**: Click them to refresh the MVR Group information manually; click the arrows to navigate to the next page or entry.

3.9 LLDP

The switch supports the LLDP. For current information on your switch model, the Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document IEEE 802.1AB.

3.9.1 LLDP Configuration

When you change LLDP configuration and the detail parameters, the settings will take effect immediately. This page enables you to view and configure the current LLDP port settings.

Web Interface

To configure LLDP:

1. Click LLDP configuration.
2. Modify the LLDP timing parameters.
3. Set the required mode for transmitting or receiving LLDP messages.
4. Specify the information to include in the TLV field of advertised messages.
5. Click Save.

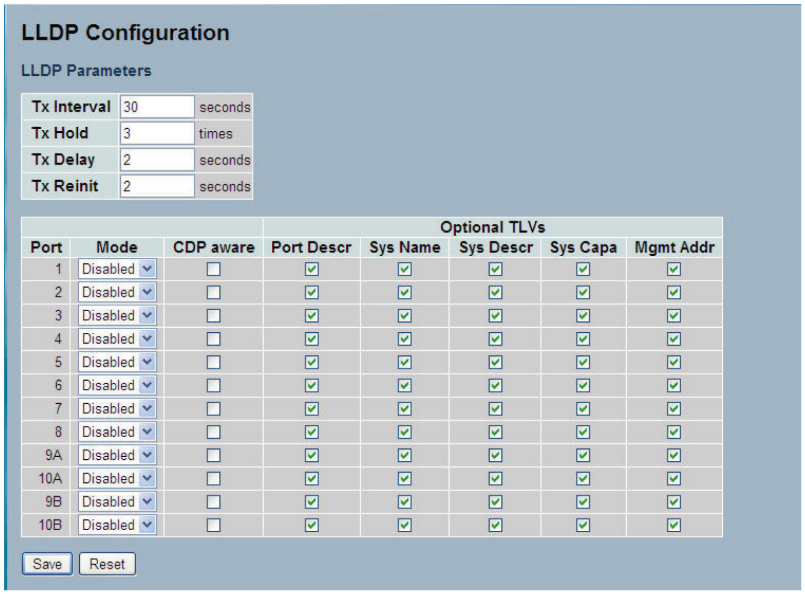


Figure 3-43: The LLDP Configuration screen.

Parameter Description

LLDP Parameters

- **Tx Interval**: The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to five to 32768 seconds.
- **Tx Hold**: Each LLDP frame contains information about how long the information in the LLDP frame will be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to two to 10 times.

- Tx Delay: If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to one to 8192 seconds.
- Tx Reinit: When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to one to 10 seconds.

LLDP Port Configuration

The LLDP port settings relate to the one that is currently selected, as shown in the page header.

- Port: The switch port number of the logical LLDP port.
- Mode: Select LLDP mode.
  - Rx only: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
  - Tx only: The switch will drop LLDP information received from neighbors, but will send out LLDP information.
  - Disabled: The switch will not send out LLDP information, and will drop LLDP information received from neighbors.
  - Enabled: The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
- CDP Aware:

Select CDP awareness.

- The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.
- Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded. (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.
- CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.
- CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.
- CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.
- CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.
- Both the CDP and LLDP support "system capabilities," but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.
- If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled, all CDP frames are terminated by the switch.

NOTE: When CDP awareness on a port is disabled, CDP information isn't removed until the hold time is exceeded.

- Port Descr: Optional TLV: When checked the "port description" is included in LLDP information.
- Sys Name: Optional TLV: When checked the "system name" is included in LLDP information.
- Sys Descr: Optional TLV: When checked the "system description" is included in LLDP information.
- Sys Capa: Optional TLV: When checked the "system capability" is included in LLDP information.
- Mgmt Addr: Optional TLV: When checked the "management address" is included in LLDP information.
- Buttons:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.9.2 LLDP Neighbors

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:

Web Interface

To show LLDP neighbors:

1. Click LLDP Neighbors.
2. Click Refresh for manual update Web screen.
3. Click Auto-refresh for auto-update Web screen.

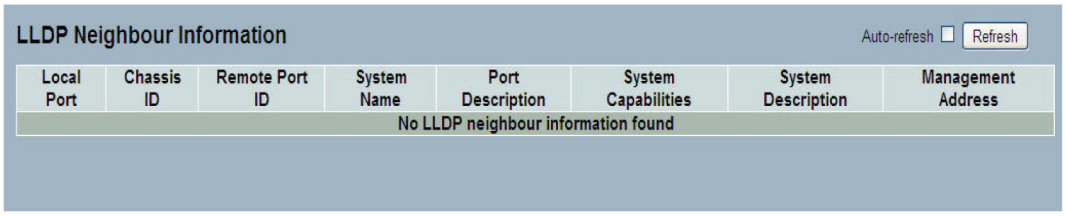


Figure 3-44: The LLDP Neighbor information screen.

NOTE: If your network supports LLDP, without any external devices connected, then the table will say "No LLDP neighbor information found".

Parameter Description

- **Local Port**: The port on which the LLDP frame was received.
- **Chassis ID**: The Chassis ID is the identification of the neighbor's LLDP frames.
- **Remote Port ID**: The Remote Port ID is the identification of the neighbor port.
- **System Name**: System Name is the name advertised by the neighbor unit.
- **Port Description**: Port Description is the port description advertised by the neighbor unit.
- **System Capabilities**: System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:
  1. Other
  2. Repeater
  3. Bridge
  4. WLAN Access Point
  5. Router
  6. Telephone
  7. DOCSIS cable device
  8. Station only
  9. Reserved

  When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

- **System Description**: System Description is the port description advertised by the neighbor unit.
- **Management Address**: Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could hold the neighbor's IP address, for example.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the LLDP Neighbors information manually.

3.9.3 LLDP-MED Configuration

Media Endpoint Discovery (MED) is an enhancement of LLDP, known as LLDP-MED, that provides the following facilities:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.
- Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.
- Extended and automated power management of Power over Ethernet (PoE) end points.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

This page enables you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Web Interface

To configure LLDP-MED:

1. Click LLDP-MED Configuration.
2. Modify the Fast start repeat count parameter. The default setting is 4.
3. Modify Coordinates Location parameters.
4. Fill Civic Address Location parameters.
5. Add the new policy.
6. Click Save, will show following Policy Port Configuration.
7. Select a Policy ID for each port.
8. Click Save.

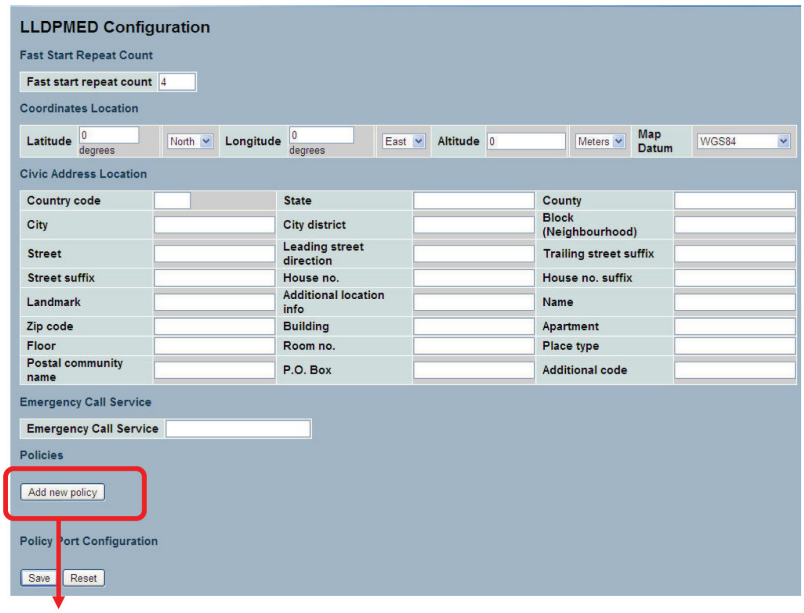


Figure 3-45. The LLDP-MED Configuration screen.

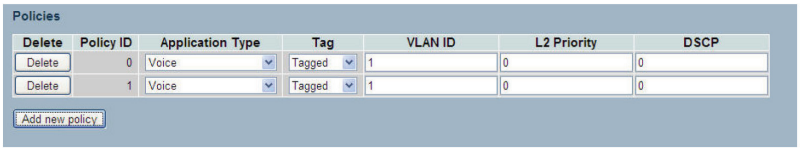


Figure 3-46. The LLDP-MED Configuration Policies screen .

Parameter Description Fast Start Repeat Count

The Rapid startup and Emergency Call Service Location Identification Discovery of endpoints are critically important aspects of VoIP systems. It is best to advertise only those pieces of information that are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind, LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second when a new LLDP-MED neighbor has been detected to share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, Black Box recommends that you repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With the fast start repeat count selection, it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1-second interval will be transmitted, when an LLDP frame with new information is received.

NOTE: The LLDP-MED and the LLDP-MED Fast Start mechanism are only intended to run on links between LLDP-MED Network connectivity Devices and Endpoint Devices, and as such do not apply to links between LAN infrastructure elements, including network connectivity devices, or other types of links.

Parameter Description: Coordinates Location

- Latitude: Latitude should be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either north of the equator or south of the equator.
- Longitude: Longitude should be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either east of the prime meridian or west of the prime meridian.
- Altitude: Altitude should be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (meters or floors).

  - Meters: Representing meters of altitude defined by the vertical data specified.

  - Floors: Representing altitude in a form more relevant in buildings that have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
- Map Datum: The Map Datum is used for the coordinates given in these options:

  - WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

  - NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich. The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

  - NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich. The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Parameter Description:

- **Civic Address Location:** IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).
- **Country code**: The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
- **State**: National subdivisions (state, canton, region, province, prefecture).
- **County**: County, parish, gun (Japan), district.
- **City**: City, township, shi (Japan) - Example: Copenhagen.
- **City district**: City division, borough, city district, ward, chou (Japan).
- **Block (Neighborhood)**: Neighborhood, block.
- **Street**: Example: Poppelvej.
- **Leading street direction**: Leading street direction - Example: N.
- **Trailing street suffix**: Example: SW.
- **Street suffix**: Example: Ave, Platz.
- **House no.**: Example: 21.
- **House no. suffix**: House number suffix - Example: A, 1/2.
- **Landmark**: Landmark or vanity address - Example: Columbia University.
- **Additional location info**: Example: South Wing.
- **Name**: (Residence and office occupant) - Example: Flemming Jahn.
- **Zip code**: Postal/zip code - Example: 2791.
- **Building**: Building (structure) - Example: Low Library.

- **Apartment**: Unit (Apartment, suite) - Example: Apt 42.
- **Floor**: Floor - Example: 4.
- **Room no.**: Room number - Example: 450F.
- **Place type**: Place type - Example: Office.
- **Postal community name**: Example: Leonia.
- **P.O. Box**: Post office box (P.O. BOX) - Example: 12345.
- **Additional code**: Example: 1320300003.
- **Emergency Call Service**: (e.g. E911 and others), such as defined by TIA or NENA.
- **Emergency Call Service**: Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Parameter Configuration:

Policies: Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service. Policies are only intended for use with applications that have specific "real-time" network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Videoconferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same network connectivity device may advertise different sets of policies, based on the authenticated user identity or port configuration.

NOTE: LLDP-MED is not intended to run on links other than between network connectivity devices and endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

- Delete: Check to delete the policy. It will be deleted during the next save.
- Policy ID: ID for the policy. This is auto generated and should be used when selecting the polices that are mapped to the specific ports.

- **Application Type:** Intended use of the application types:
  1. Voice - for use by dedicated IP telephony handsets and similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
  2. Voice Signaling (conditional) - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
  3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP telephony handsets and other similar appliances supporting interactive voice services.
  4. Guest Voice Signaling (conditional) - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.
  5. Softphone Voice - for use by softphone applications on typical data-centric devices, such as PCs or laptops. This class of end points frequently does not support multiple VLANs, if at all, and are typically configured to use an "untagged" VLAN or a single "tagged" data-specific VLAN. When a network policy is defined for use with an "untagged" VLAN (see Tagged flag below), then the L2 priority field is ignored, and only the DSCP value has relevance.
  6. Videoconferencing - for use by dedicated videoconferencing equipment and other similar appliances supporting real-time interactive video/audio services.
  7. Streaming Video - for use by broadcast or multicast-based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
  8. Video Signaling (conditional) - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
- **Tag**: Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
- **VLAN ID**: VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.
- **L2 Priority**: L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
- **DSCP**: DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.
- **Adding a new policy**: Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save."
- **Port Policies Configuration**: Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.
- **Port**: The port number to which the configuration applies.
- **Policy ID**: The set of policies that apply to a given port. Set policies by checking the corresponding checkboxes.
- **Buttons**: "Save": Click to save changes; "Reset": Click to undo any changes made locally and revert to previously saved values.

3.9.4 LLDP-MED Neighbors

This section provides a status overview of all LLDP-MED neighbors. The table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices that support LLDP-MED.

Web Interface

To show LLDP-MED neighbor:

1. Click LLDP-MED Neighbor.
2. Click Refresh for manual update Web screen.
3. Click Auto-refresh for auto-update Web screen.

Figure 3-47: The LLDP-MED Neighbor Information screen

NOTE: If your network supports LLDPMED without any devices, then the table will show "No LLDP-MED neighbor information found".

Parameter Description

- **Port**: The port on which the LLDP frame was received.
- **Device Type**:
  - LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.
  - LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802-based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

  1. LAN Switch/Router
  2. IEEE 802.1 Bridge
  3. IEEE 802.3 Repeater (included for historical reasons)
  4. IEEE 802.11 Wireless Access Point
  5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

- **LLDP-MED Endpoint Device Definition**:

  LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

  Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

- **LLDP-MED Generic Endpoint (Class I)**: The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

  Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

- **LLDP-MED Media Endpoint (Class II)**: The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) voice / media gateways, conference bridges, media servers, etc.

  Discovery services defined in this class include media-type-specific network layer policy discovery.

- **LLDP-MED Communication Endpoint (Class III)**: The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all those defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

  Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

- **LLDP-MED Capabilities**: LLDP-MED Capabilities describes the neighborhood unit's LLDP-MED capabilities. The possible capabilities are:

  1. LLDP-MED capabilities

  2. Network Policy

  3. Location Identification

  4. Extended Power via MDI - PSE

  5. Extended Power via MDI - PD

  6. Inventory

  7. Reserved

- **Application Type**: Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below:

  1. Voice - for use by dedicated IP telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

  2. Voice Signaling - for use in network topologies that require a different policy for the voice signaling than for the voice media.

  3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP telephony handsets and other similar appliances supporting interactive voice services.

  4. Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.

  5. Softphone Voice - for use by softphone applications on typical data-centric devices, such as PCs or laptops.

  6. Videoconferencing - for use by dedicated videoconferencing equipment and other similar appliances supporting real-time interactive video/audio services.

7. Streaming Video - for use by broadcast or multicast-based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signaling - for use in network topologies that require a separate policy for the video signaling than for the video media.

- Policy: Policy indicates that an endpoint device wants to explicitly advertise that the policy is required by the device. It can be either Defined or Unknown.
  - Unknown: The network policy for the specified application type is currently unknown.
  - Defined: The network policy is defined.
- TAG: TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. It can be Tagged or Untagged.
  - Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.
  - Tagged: The device is using the IEEE 802.1Q tagged frame format.
- VLAN ID: VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
- Priority: Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
- DSCP: DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

3.9.5 PoE

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each port on which an LLDP PoE neighbor is detected. The columns hold the following information:

Web Interface

To show LLDP PoE neighbors:

1. Click LLDP, then click PoE to show discovered PoE devices.
2. Click Refresh to go to the manual update Web screen.
3. Click Auto-refresh to auto-update the screen.

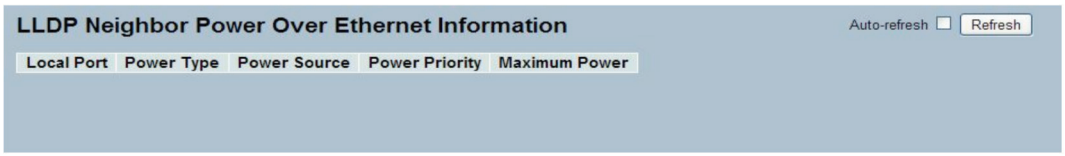


Figure 3-48: The LLDP neighbors PoE information

NOTE: If your network without any PoE device supports LLDP-MED, then the table will show "blank."

Parameter Description

- **Local Port:** The port for this switch on which the LLDP frame was received.
- **Power Type:** The type represents whether the device is Power Sourcing Equipment (PSE) or a Powered Device (PD). If the type is unknown, it is represented as "Reserved."
- **Power Source:** The power source used by PSE or a PD.

  If the device is PSE, it can either run on its primary power source or its backup power source. If it is unknown whether or not the PSE device is using its primary power source or its backup power source, the screen displays "Unknown." If the device is a PD, it can either run on its local power supply or it can use the PSE as a power source. It can also use both its local power supply and the PSE. If it is unknown what power supply the PD is using, it is indicated as "Unknown."
- **Power Priority:** Power priority represents the priority of the PD or the power priority associated with PSE type device's port that is sourcing the power. There are three levels of power priority: Critical, High, and Low. If the power priority is unknown, it is indicated as "Unknown."
- **Maximum Power:** This indicates the maximum power in watts required by a PD from PSE, or the minimum power PSE is capable of sourcing over a maximum-length cable based on its current configuration. The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "Reserved."
- **Auto-refresh:** Check the auto-refresh box to set the unit to refresh the information automatically.
- **Icons, upper right or screen (Refresh, <<, >>):** Click them to refresh the LLDP neighbors information manually.

3.9.6 EEE

By using EEE, power savings can be achieved at the expense of traffic latency. This latency occurs because EEE circuits turn off to save power, and they need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wakeup time" as a way to agree upon the minimum wakeup time they need. This section provides an overview of EEE and LLDP interactions.

Web Interface

To show LLDP EEE neighbors:

1. Click LLDP, then click EEE to show discover EEE devices.
2. Click Refresh for manual update Web screen.
3. Click Auto-refresh for auto-update Web screen.

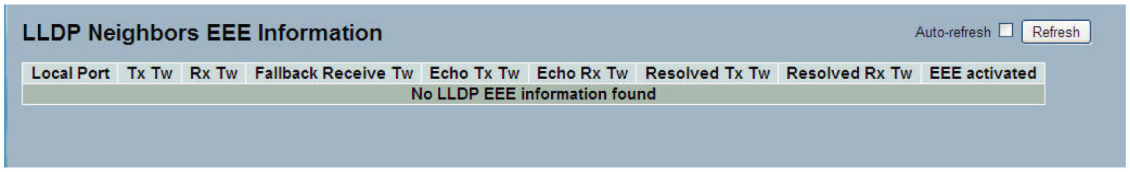


Figure 3-49. The LLDP Neighbors EEE Information screen.

NOTE: If your network has no devices that enable the EEE function, the table will show "No LLDP EEE information found."

Parameter Description

- **Local Port**: The port on which LLDP frames are received or transmitted.
- **Tx Tw**: The link partner's maximum time that transmit path can hold off sending data after reassertion of LPI.
- **Rx Tw**: The link partner's time that receiver would like the transmitter to hold off to allow time for the receiver to wake from sleep.
- **Fallback Receive Tw**: The link partner's fallback receive Tw.

  A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.
- **Echo Tx Tw**: The link partner's Echo Tx Tw value.

  The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner, it can determine whether or not the remote link partner has received, registered, and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.
- **Echo Rx Tw**: The link partner's Echo Rx Tw value.
- **Resolved Tx Tw**: The resolved Tx Tw for this link. Note: NOT the link partner The resolved value that is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).
- **Resolved Rx Tw**: The resolved Rx Tw for this link. Note: NOT the link partner The resolved value that is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon (refresh), upper right of screen**: Click to refresh the LLDP Neighbors information manually.

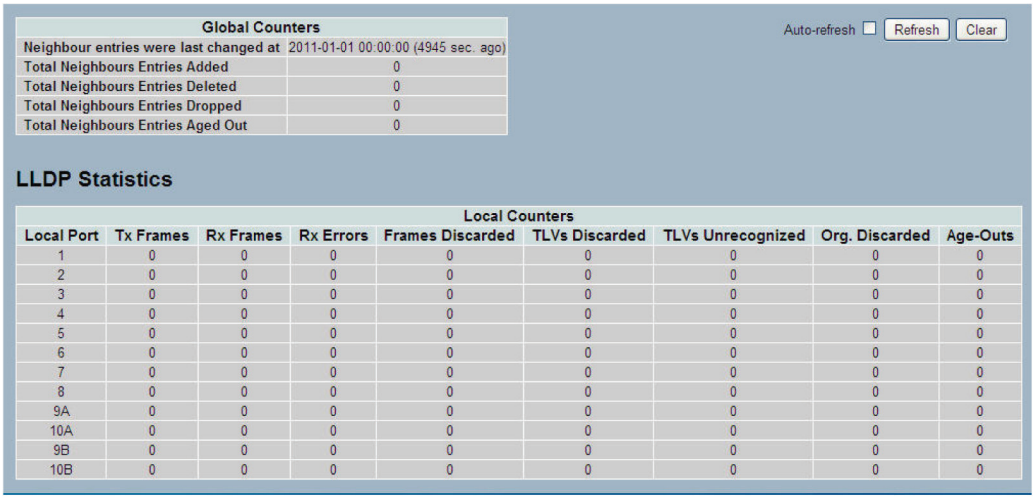
3.9.7 Port Statistics

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per-port counters for the currently selected switch.

Web Interface

To show LLDP Statistics:

1. Click LLDP, than click Port Statistics to show LLDP counters.
2. Click Refresh to see the manual update Web screen.
3. Click Auto-refresh to see the auto-update Web screen.
4. Click Clear to clear all counters.



Global Counters	
Neighbour entries were last changed at	2011-01-01 00:00:00 (4945 sec. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

Auto-refresh Refresh Clear

LLDP Statistics

Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9A	0	0	0	0	0	0	0	0
10A	0	0	0	0	0	0	0	0
9B	0	0	0	0	0	0	0	0
10B	0	0	0	0	0	0	0	0

Figure 3-50: The LLDP Port Statistics Information screen.

Parameter Description:

Global Counters

- **Neighbor entries were last changed at**: Indicates the time when the last entry was last deleted or added. It also indicates the time elapsed since the last change was detected.
- **Total Neighbors Entries Added**: Shows the number of new entries added since switch reboot.
- **Total Neighbors Entries Deleted**: Shows the number of new entries deleted since switch reboot.
- **Total Neighbors Entries Dropped**: Shows the number of LLDP frames dropped because of the entry table being full.
- **Total Neighbors Entries Aged Out**: Shows the number of entries deleted because of Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

- **Local Port**: The port on which LLDP frames are received or transmitted.
- **Tx Frames**: The number of LLDP frames transmitted on the port.
- **Rx Frames**: The number of LLDP frames received on the port.
- **Rx Errors**: The number of received LLDP frames containing an error.

- **Frames Discarded**: If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry times out.
- **TLVs Discarded**: Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
- **TLVs Unrecognized**: The number of well-formed TLVs, but with an unknown type value.
- **Org. Discarded**: The number of organizationally received TLVs.
- **Age-Outs**: Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icons, upper right of screen (Refresh, Clear)**: Click to refresh the LLDP Port Statistics information manually. Click Clear to remove any current changes you have made.

3.10 PoE

Power over Ethernet (PoE) is used to transmit electrical power to remote devices over standard Ethernet cable. Use it to power IP telephones, wireless LAN access points, and other equipment, where it would be difficult or expensive to connect the equipment to a power supply.

3.10.1 Configuration

From this page, you can inspect and configure the current PoE port settings.

Web Interface

To configure Power over Ethernet in the Web interface:

1. Click "Configuration."
2. Specify the reserved power determined and power management mode. Specify PoE or PoE+ and priority.
3. Click "Save."

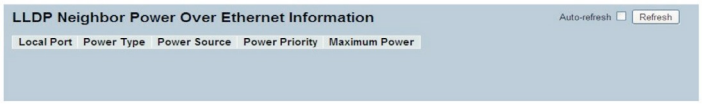


Figure 3-51. The Power over Ethernet Configuration screen.

Parameter Description

Power Supply Configuration:

- **Primary Power Supply (Watts):** The switches are used as Power Sourcing Equipment (PSE). The LPB2810A switch delivers 130 watts of PoE, the LPB2826A provides 185 Watts of PoE and the LPB2848A provides 370 watts of PoE.

Ethernet Port Configuration:

- **Port:** This is the logical port number for this row.
- **PoE State:** The PoE Mode represents the PoE operating mode for the port.

  Disabled: PoE disabled for the port.

  Enabled : Enables PoE IEEE 802.3af/at is enabled for the port.

- **Priority:** Select from three levels of power priority: Low, High, and Critical.

  The switch uses priority if remote devices require more power than the power supply can deliver. In this case, the port with the lowest priority will turn off. If more power is still needed, the next higher priority port number will turn off.

- **Maximum Power:** This is the maximum power in watts that can be delivered to a remote device.

NOTE: To set the port to support IEEE 802.3at, the maximum allowed value is 30 watts.

- **Buttons:**

  Save: Click to save changes.

  Reset: Click to undo any changes made locally and revert to previously saved values.

3.10.2 Status

The Status page allows the user to inspect the current status for all PoE ports.

Web Interface:

To display Power over Ethernet status in the Web interface:

1. Click "Status."
2. Select Display Power over Ethernet Status Information.
3. Click "Refresh."

Power Over Ethernet Status

Auto-refresh ☐ Refresh

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
2	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
3	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
4	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
5	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
6	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
7	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
8	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Figure 3-52. The Power over Ethernet Status screen.

Parameter Description

- **Local Port:** This is the logical port number for this row.
- **PD Class:** This describes the amount of power the Powered Device (PD) will require during normal operation.
- **Power Requested:** Shows the requested amount of power the PD wants to reserve.
- **Power Allocated:** Shows the amount of power the switch has allocated for the PD.
- **Power Used:** Shows how much power in watts the PD is using.
- **Current Used:** Shows how much current in mA the PD is using.
- **Priority:** Shows the port's priority configured by the user.
- **Port Status:** Shows the port's status.

- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icons, upper right of screen (Refresh)**: Click to refresh the PoE information manually.

3.11 Filtering Data Base

The Filtering Data Base Configuration function gathers many functions, including MAC Table Information, Static MAC Learning, which cannot be categorized to some function type.

MAC Table

The switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports. The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

3.11.1 Configuration

Configure the MAC Address Table on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

Web Interface

To configure MAC Address Table in the Web interface:

Aging Configuration

1. Click Configuration.
2. Specify the Disable Automatic Aging and Aging Time.
3. Click Save.

MAC Table Learning

1. Click Configuration.
2. Specify the Port Members (Auto, Disable, Secure).
3. Click Save.

Static MAC Table Configuration

1. Click Configuration and Add New Static Entry.
2. Specify the VLAN IP and Mac Address, Port Members.
3. Click Save.

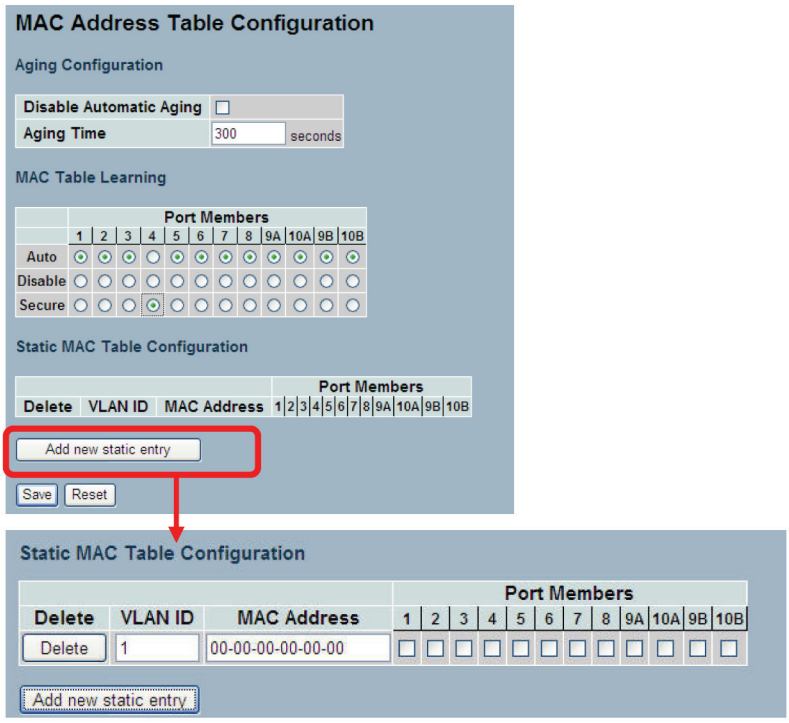


Figure 3-53: The MAC Address Table Configuration screen.

Parameter Description

- Aging Configuration: By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

  Configure aging time by entering a value here in seconds. For example, Age time seconds.

  The range given should be 10 to 1,000,000 seconds.

  Disable the automatic aging of dynamic entries by checking Disable Automatic Aging.

MAC Table Learning Mode

If the Learning Mode for a given port is grayed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X. Each port can "learn" based upon the following settings:

- **Auto**: Learning is done automatically as soon as a frame with unknown SMAC is received.
- **Disable**: No learning is done.
- **Secure**: Only static MAC entries are learned, all other frames are dropped.

NOTE: Make sure that the link used for managing the switch is added to the Static MAC Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The MAC table is sorted first by VLAN ID and then by MAC address.

- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **VLAN ID**: The VLAN ID of the entry.
- **MAC Address**: The MAC address of the entry.
- **Port Members**: Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
- **Add a New Static Entry**: Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.11.2 Dynamic MAC Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries and is sorted first by VLAN ID then by MAC address.

Web Interface

To Display MAC Address Table in the Web interface:

1. Click Dynamic MAC Table.
2. Specify the VLAN and MAC Address.
3. Display MAC Address Table.

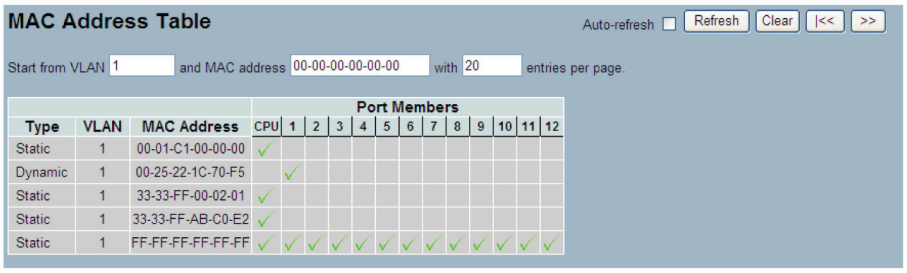


Figure 3-54. The Dynamic MAC Address Table information screen.

Parameter Description

MAC Table Columns

- **Type**: Indicates whether the entry is a static or a dynamic entry.
- **VLAN**: The VLAN ID of the entry.
- **MAC Address**: The MAC address of the entry.
- **Port Members**: The ports that are members of the entry.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icons, upper right (Refresh, Clear, <<, >>)**: Click to refresh the MAC address manually. Press Clear to clear all new entries from the MAC table. Press << or >> to scroll to the next entry on the table.

NOTE the following MAC addresses:

00-40-C7-73-01-29: your switch MAC address (for IPv4).

33-33-00-00-00-01: Destination MAC (for IPv6 Router Advertisement) (reference IPv6 RA.JPG).

33-33-00-00-00-02: Destination MAC (for IPv6 Router Solicitation) (reference IPv6 RS.JPG).

33-33-FF-73-01-29: Destination MAC (for IPv6 Neighbor Solicitation) (reference IPv6 DAD.JPG).

33-33-FF-A8-01-01: your switch MAC address (for IPv6 global IP).

FF-FF-FF-FF-FF-FF: for Broadcast.

3.12 VLAN

This section describes how to assign a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN by configuring System->IP->IPv4->VLAN ID. Only one management VLAN can be active at a time.

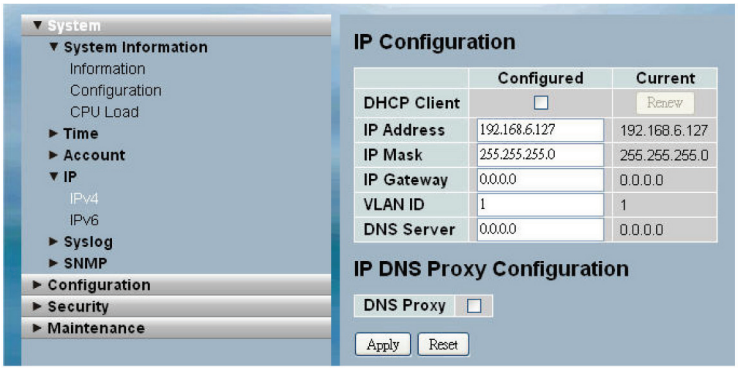


Figure 3-55. IP Configuration for management VLAN screen.

When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route.

3.12.1 VLAN Membership

The VLAN membership configuration for the selected switch can be monitored and modified here. Up to 4094 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

Web Interface

To configure VLAN membership configuration in the Web interface:

1. Click VLAN Membership Configuration.
2. Specify a Management VLAN ID from 1~ 4094.
3. Click Save.

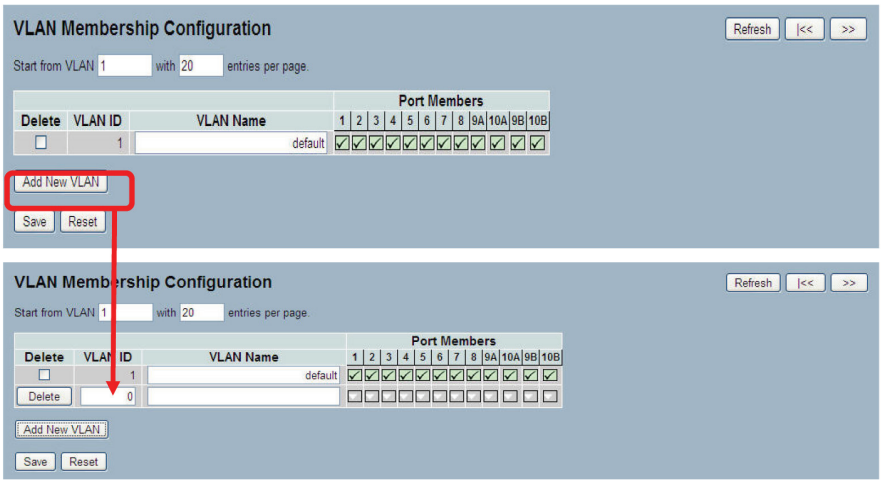


Figure 3-56. The VLAN Membership Configuration screen.

Parameter Description

- **Delete**: To delete a VLAN entry, check this box and the entry will be deleted on the selected switch.

WARNING: the default VLAN 1 can be deleted. But if deleting the default VLAN 1, the connection to the switch would be lost and some errors would occur.

- **VLAN ID**: Indicates the ID of every single VLAN. Legal values for a VLAN ID are 1 to 4094.
- **VLAN Name**: Indicates the name of VLAN. VLAN Name can contain letters, numbers, or a mix of letters and numbers, but excludes special characters. VLAN Name can leave blanks. The length of VLAN name supports up to 32 characters. VLAN name can be edited for the existing VLAN entries.
- **Port Members**: A row of checkboxes for each port display port members of each VLAN. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked.
- **Adding a New VLAN**: Click to add a new VLAN group. An empty row, no port is a member, and all boxes are unchecked, is added to the table to configure. A VLAN without any port members can not be set up.
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

- **Icons, upper right (Refresh, |<<, >>)**: Click to refresh the MAC address manually. Press |<< or >> to scroll to the next entry on the table.

3.12.2 Ports

User can configure all parameters to each port in VLAN Port Setting. These parameters involved two parts, Ingress rule and Egress rule. The function of Port Type, Ingress Filtering, Frame Type, and PVID affect Ingress process. Furthermore, Port Type, Egress Rule, and PVID affect Egress process.

Web Interface

To configure VLAN Port configuration in the Web interface:

1. Click VLAN Port Configuration.
2. Specify the VLAN Port Configuration parameters.
3. Click Save.

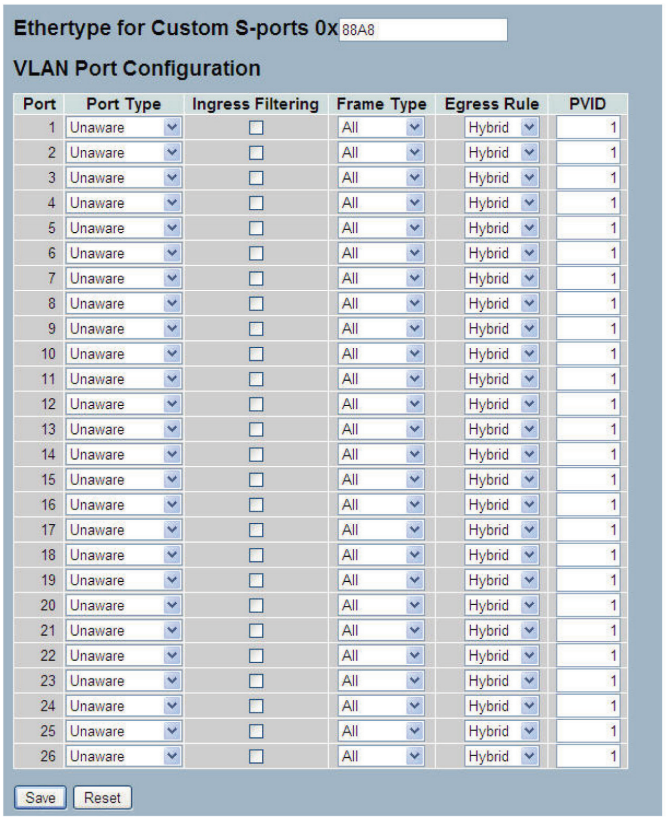


Figure 3-57. The VLAN Port Configuration screen.

Parameter Description

- **Ethertype for Custom S-ports**: This field specifies the ether type used for Custom S-ports while s-custom-port enabled. This is a global setting for all the Custom S-ports. Custom Ethertype enables the user to change the Ethertype value on a port to any value to support network devices that do not use the standard 0x8100 Ethertype field value on 802.1Q-tagged or 02.1P-tagged frames.
- **Port**: Indicate the port number of each port.
- **Port Type**: A port can be one of the following types: Unaware, C-port, S-port, and S-custom-port.

Table 3-1: Port Types.

Port Type	Ingress Action	Egress Action
Unaware: The function of Unaware can be used for 802.1QinQ (double tag).	When the port received untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port received tagged frames, 1. if the tagged frame with TPID=0x8100, it becomes a double-tag frame, and is forwarded. 2. if the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of a frame transmitted by an Unaware port will be set to 0x8100.
C-port	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port received tagged frames: 1. if an tagged frame with TPID=0x8100, it is forwarded. 2. if the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by the C-port will be set to 0x8100.
S-port	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port received tagged frames: 1. if an tagged frame with TPID=0x88A8, it is forwarded. 2. if the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID of frame transmitted by S-port will be set to 0x88A8.
S-custom-port	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded. When the port received tagged frames: 1. if an tagged frame with TPID=0x88A8, it is forwarded. 2. if the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID of frame transmitted by S-custom-port will be set to an self-customized value, which can be set by the user using the column of Ethertype for Custom S-ports.

- **Ingress Filtering**: Enable ingress filtering on a port by checking the box. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN group of the frame, the frame is discarded (Do not forward). If ingress filtering is disabled and the ingress port is not a member of the classified VLAN group of the frame, however, the frame is still forwarded. By default, ingress filtering is disabled (untick).
- **Frame Type**: Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.
- **Egress Rule**: Determines what device the port connect to. If the port connect to VLAN-unaware devices, such as terminal/workstation, Access link should be used. If the port connects to VLANaware devices, for example, switch connect to switch, Trunk link should be used. The Hybrid link is used for more flexible applications.

  Hybrid: If the tag of tagged frame is as the same as PVID, the tag of the frame will be removed. The frame becomes an untagged frame and transmitted. Any other tagged frame whose tag value is different from PVID are transmitted directly.

  Trunk: All tagged frames with any tag value are transmitted.

  Access: The tag of any tagged frame will be removed to become an untagged frame. These untagged frames will be transmitted.
- **PVID**: Configures the Port VLAN identifier. The acceptable values are 1 through 4094. The default value is 1. When the port receives a untagged frame, the port will give a tag to it based on the value of PVID, and the frame becomes a tagged frame.

NOTE: The port must be a member of the same VLAN as the Port VLAN ID.

3.12.3 Switch Status

The function Switch Status gathers the information of all VLAN status and reports it by the order of Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.

Web Interface

To Display VLAN membership status in the Web interface:

1. Click VLAN membership.
2. Specify the Staic NAS MVRP MVP Voice VLAN MSTP GVRP Combined.
3. Display membership information.

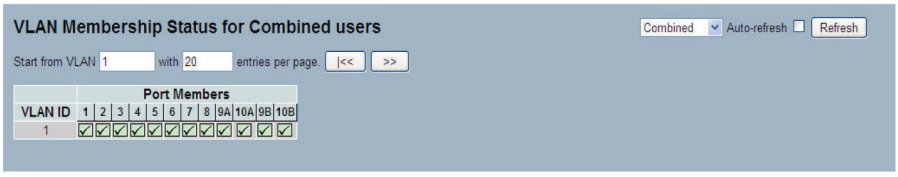


Figure 3-58. The VLAN Membership Status for Combined Users screen.

Parameter Description

VLAN User (Scroll to select the type of VLAN user):

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types:

CLI/Web/SNMP: These are referred to as static.

NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

MVRP: Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

GVRP: GARP VLAN Registration Protocol (GVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

Voice VLAN: Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.

MVR: MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

MSTP: The 802.1s Multiple Spanning Tree protocol (MSTP). It uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

- **VLAN ID**: Indicates the ID of this particular VLAN.
- **VLAN Membership**: The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users are selected, it shall show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the LLDP Neighbors information manually.

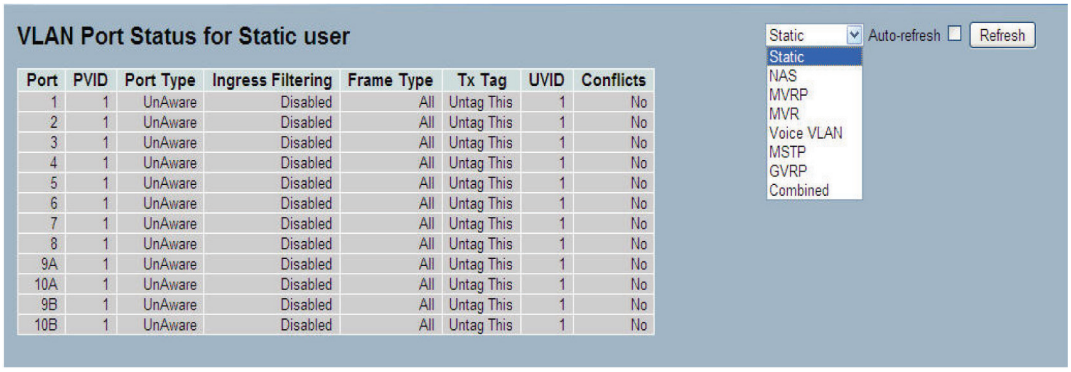
3.12.4 Port Status

This function, Port Status, gathers the information of all VLAN status and reports it by the order of Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.

Web Interface

To Display VLAN Port Status in the Web interface:

1. Click VLAN Port Status.
2. Specify the Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.
3. Display Port Status information.



Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag This	1	No
2	1	UnAware	Disabled	All	Untag This	1	No
3	1	UnAware	Disabled	All	Untag This	1	No
4	1	UnAware	Disabled	All	Untag This	1	No
5	1	UnAware	Disabled	All	Untag This	1	No
6	1	UnAware	Disabled	All	Untag This	1	No
7	1	UnAware	Disabled	All	Untag This	1	No
8	1	UnAware	Disabled	All	Untag This	1	No
9A	1	UnAware	Disabled	All	Untag This	1	No
10A	1	UnAware	Disabled	All	Untag This	1	No
9B	1	UnAware	Disabled	All	Untag This	1	No
10B	1	UnAware	Disabled	All	Untag This	1	No

Figure 3-59. The VLAN Port Status for Static User screen.

Parameter Description

- **Port**: The logical port for the settings contained in the same row.
- **PVID**: Shows the VLAN identifier for that port. The acceptable values are 1 through 4095. The default value is 1.
- **Port Type**: Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port.

  If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.
- **Ingress Filtering**: Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.
- **Frame Type**: Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames; untagged frames received on that port are discarded.
- **Tx Tag**: Shows egress filtering frame status whether tagged or untagged.
- **UVID**: Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.
- **Conflicts**: Shows status of Conflicts whether exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

  - Functional Conflicts between features.

  - Conflicts from hardware limitation.

  - Direct conflict between user modules.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the VLAN Port Status information manually.

3.12.5 Private VLANs

In a private VLAN, communication between ports is not permitted. A VLAN can be configured as a private VLAN.

Assigning Membership in Private VLANs

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Web Interface

To configure Private VLAN configuration in the Web interface:

1. Click add new Private VLAN configuration
2. Specify the Private VLAN ID and Port Members
3. Click Save.

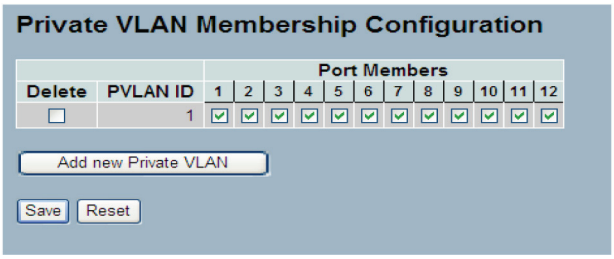


Figure 3-60. The Private VLAN Membership Configuration screen.

Parameter Description

- **Delete**: To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
- **Private VLAN ID**: Indicates the ID of this particular private VLAN.
- **Port Members**: A row of checkboxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
- **Adding a New Private VLAN**: Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

Port Isolation

Port Isolation provides for an apparatus and method to isolate ports on Layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map, which is responsive to a destination address of a data packet. The method for isolating ports on a Layer 2 switch comprises configuring each of the ports on the Layer 2 switch as a protected port or a non-protected port. A destination address on a data packet is matched with a physical address on that Layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

This section describes how to enable and disable port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Web Interface

To configure Port Isolation configuration in the Web interface:

1. Click VLAN, Port Isolation.
2. Check the box of the port for which you want to enable Port Isolation.
3. Click Save.

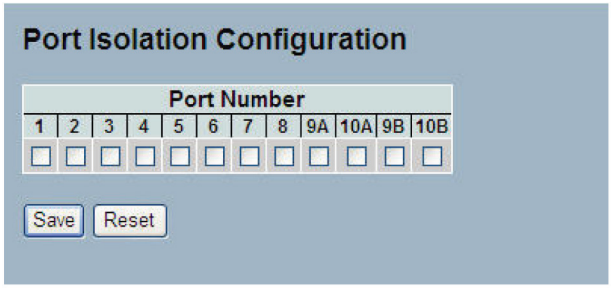


Figure 3-61. The Port Isolation Configuration screen.

Parameter Description

- **Port Number**: A checkbox is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.12.6 MAC-Based VLAN

MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

A most common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure, and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. To provide user access and ensure data security in the meantime, the MAC-based VLAN technology is developed.

MAC-based VLANs group VLAN members by MAC address.

With MAC-based VLAN configured, the device adds a VLAN tag
to an untagged frames according to its source MAC address. MAC-based VLANs are mostly used with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

Configuration

The MAC-based VLAN enties can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Web Interface

To configure MAC address-based VLAN configuration in the Web interface:

1. Click MAC address-based VLAN configuration and add new entry.
2. Specify the MAC address and VLAN ID.
3. Click Save.

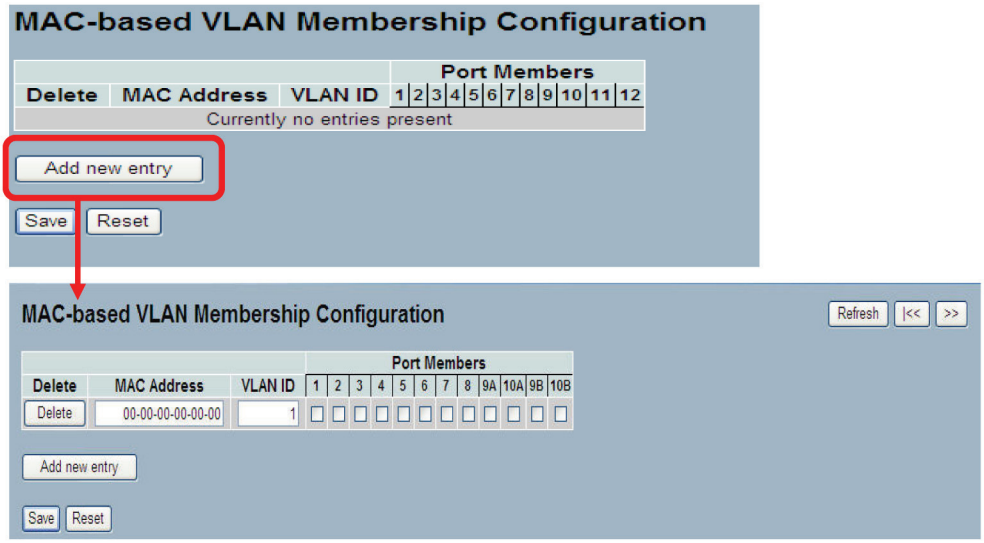


Figure 3-62. The MAC-Based VLAN Membership Configuration screen.

Parameter Description

- **Delete**: To delete a MAC-based VLAN entry, check this box and press Save. The entry will be deleted on the selected switch.
- **MAC Address**: Indicates the MAC address.
- **VLAN ID**: Indicates the VLAN ID.
- **Port Members**: A row of checkboxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
- **Adding a New MAC-based VLAN**: Click to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095.

  The MAC-based VLAN entry is enabled on the selected switch unit when you click on "Save." A MAC-based VLAN without any port members on any unit will be deleted when you click "Save." The buttons can be used to undo the addition of new MAC-based VLANs.
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

Status

This section shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:

NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

Web Interface

To Display MAC-based VLAN configured in the Web interface:

1. Click MAC-based VLAN Status.
2. Specify the Static NAS Combined.
3. Display MAC-based information.

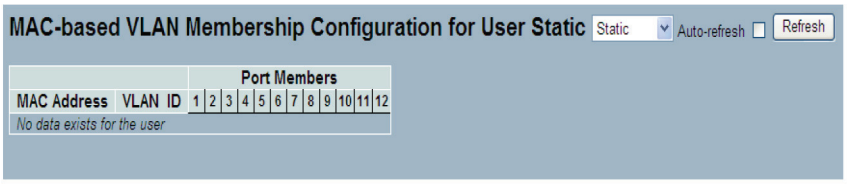


Figure 3-63. The MAC-based VLAN Membership Status for User Static screen.

Parameter Description

- MAC Address: Indicates the MAC address.
- VLAN ID: Indicates the VLAN ID.
- Port Members: Port members of the MAC-based VLAN entry.
- Auto-refresh: Check the auto-refresh box to set the unit to refresh information automatically.
- Icon, upper right of screen (Refresh): Click to refresh the MAC-based VLAN Memebership information manually.

3.12.7 Protocol-Based VLAN

This section describes Protocol-based VLAN. The switch supports protocol including Ethernet LLC SNAP Protocol.

LLC

The Logical Link Control (LLC) data communications protocol layer is the upper sub-layer of the Data Link Layer (which is itself Layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, DecNet, and AppleTalk®) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP

The Subnetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

Protocol to Group

This section describes how to add new protocols to Group Name (unique for each Group) mapping entries and to see and delete already-mapped entries for the selected switch.

Web Interface

To configure protocol-based VLAN configuration in the Web interface:

1. Click protocol-based VLAN configuration and add new entry.
2. Specify the Ethernet LLC SNAP Protocol and Group Name.
3. Click Save.

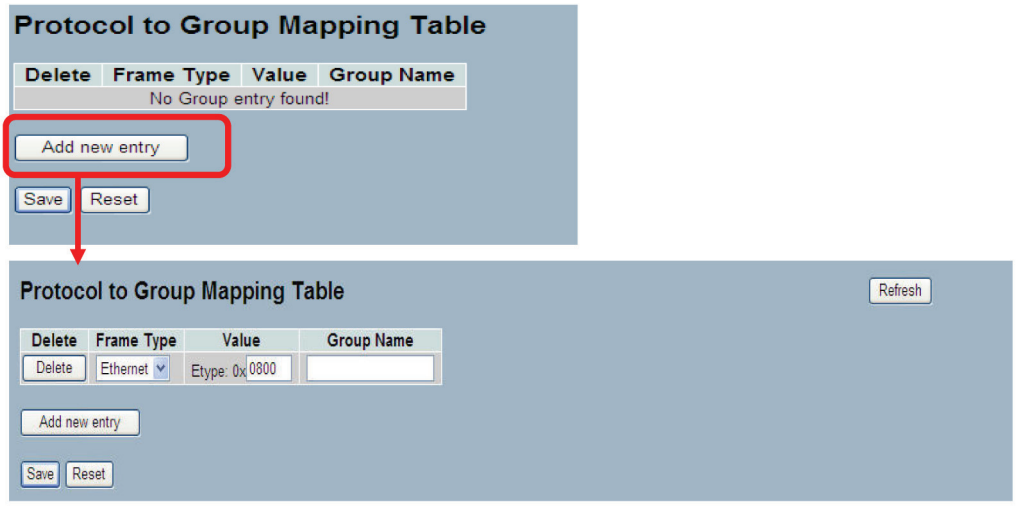


Figure 3-64. The Protocol to Group Mapping Table screen.

Parameter Description

- **Delete**: To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.
- **Frame Type**: Frame Type can have one of the following values:

  1. Ethernet

  2. LLC

  3. SNAP

NOTE: When you change the Frame type field, the valid value of the following text field will vary depending on the new frame type you selected.

- **Value**: The valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.

  Below are the criteria for three different Frame Types:

  1. For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff

  2. For LLC: Valid value in this case is comprised of two different sub-values.

  a. DSAP: 1-byte long string (0x00-0xff)

  b. SSAP: 1-byte long string (0x00-0xff)

  3. For SNAP: Valid value in this case also is comprised of two different sub-values.

  a.OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx whereeach pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.

  b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

  In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

- **Group Name**: A valid Group Name is a unique 16-character long string for every entry. Entries should consist of a combination of letters (a-z or A-Z) and numbers (0-9).

NOTE: Special character and underscore (_) are not allowed.

- **Adding a New Group to VLAN mapping entry**: Click to add a new entry in the mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed. The Reset button can be used to undo the addition of a new entry.
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

- **Icon, upper right (Refresh)**: Click to refresh the Protocol Group Mapping information manually.

Group to VLAN

This section has instructions on how to map an already-configured Group Name to a VLAN for the selected switch.

Web Interface

To Display Group Name to VLAN mapping table configured in the Web interface:

1. Click Group Name VLAN configuration and add new entry.
2. Specify the Group Name and VLAN ID.
3. Click Save.

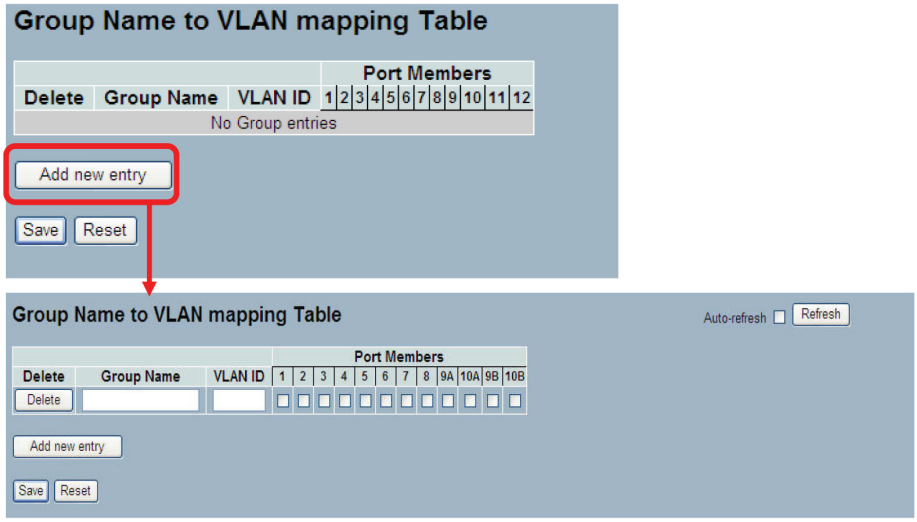


Figure 3-65. The Group Name of VLAN Mapping Table screen.

Parameter Description

- **Delete**: To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save
- **Group Name**: A valid Group Name is a string of atmost 16 characters which consists of a combination of letters (a-z or A-Z) and numbers (0-9). No special characters are allowed. Any Group names you try to map to a VLAN must be present in Protocol to Group mapping table and must not be used by any other existing mapping entry on this page.
- **VLAN ID**: Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
- **Port Members**: A row of checkboxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
- **Adding a New Group to VLAN mapping entry**: Click to add a new entry in mapping table. An empty row is added to the table, and the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The Reset button can be used to undo the addition of new entry.
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the Protocol Group Mapping information manually.

3.13 Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

3.13.1 Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port—one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Web Interface

To configure Voice VLAN in the Web interface:

1. Select "Enabled" in the Voice VLAN Configuration.
2. Specify VLAN ID Aging Time Traffic Class.
4. Specify (Port Mode, Security, Discovery Protocol) in the Port Configuration.
5. Click Save.

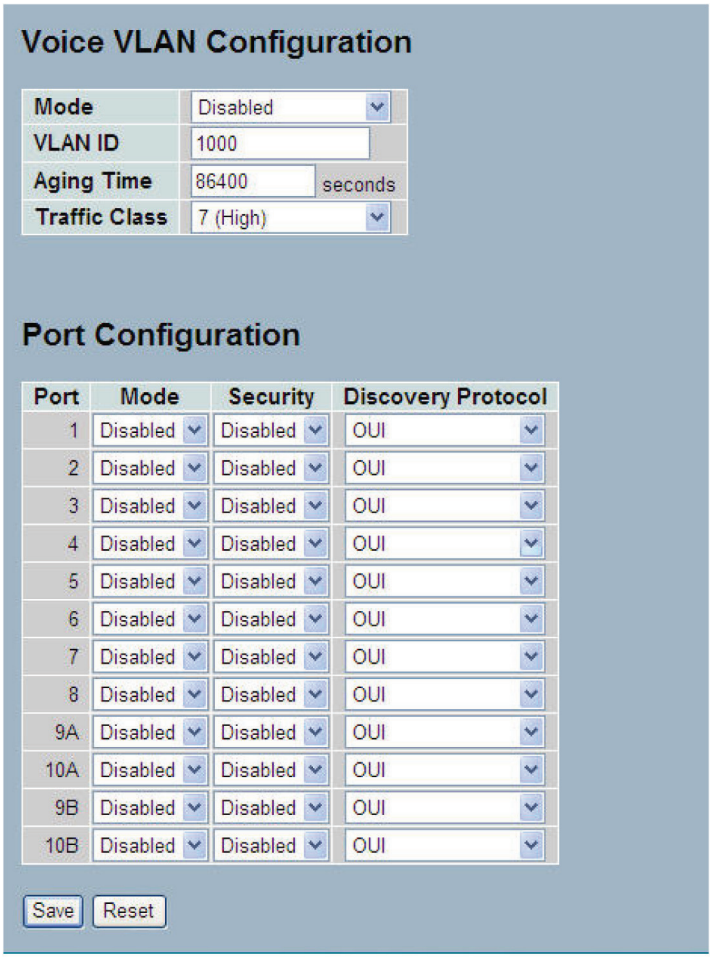


Figure 3-66. The Voice VLAN Configuration screen.

Parameter Description

- **Mode**: Indicates the Voice VLAN mode operation. Disable the MSTP feature before enabling Voice VLAN to avoid the conflict of ingress filtering. Possible modes are:

  Enabled: Enable Voice VLAN mode operation.

  Disabled: Disable Voice VLAN mode operation.

- **VLAN ID**: Indicates the Voice VLAN ID. This should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The valid range is 1 to 4095.

- **Aging Time**: Indicates the Voice VLAN secure learning aging time. The range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

- **Traffic Class**: Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply to this class.

- **Port Mode**: Indicates the Voice VLAN port mode. When the port mode isn't equally disabled, first disable MSTP feature before enabling Voice VLAN, to avoid the conflict of ingress filtering.

  Possible port modes are:

  Disabled: Disjoin from Voice VLAN.

  Auto: Enable auto detect mode to detect whether there is a VoIP phone attached to the specific port. This mode configures the Voice VLAN members automatically.

  Forced: Force join to Voice VLAN.

- **Port Security**: Indicates the Voice VLAN port security mode. When the function is enabled, all nontelephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

  Enabled: Enable Voice VLAN security mode operation.

  Disabled: Disable Voice VLAN security mode operation.

- **Port Discovery Protocol**: Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. Enable the LLDP feature before configuring discovery protocol to "LLDP" or "Both." Changing the discovery protocol to "OUI" or "LLDP" will restart the autodetect process. Possible discovery protocols are:

  OUI: Detect telephony device by OUI address.

  LLDP: Detect telephony device by LLDP.

  Both: Both OUI and LLDP.

- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.13.2 OUI

This section describes how to Configure the VOICE VLAN OUI table. The maximum entry number is 16. Modifying the OUI table will restart auto detection of OUI process.

Web Interface

To configure Voice VLAN OUI Table in the Web interface:

1. Select "Add new entry", then check "Delete" in the Voice VLAN OUI table.
2. Specify Telephony OUI, Description.
3. Click Save.

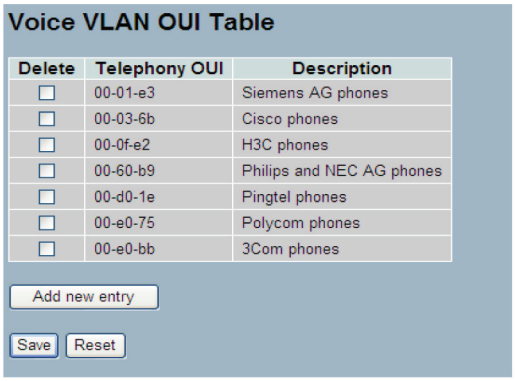


Figure 3-67. The Voice VLAN OUI Table screen.

Parameter Description

- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **Telephony OUI**: A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
- **Description**: The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The string length should fall between 0 and 32.
- **Add New entry**: Click to add a new entry in Voice VLAN OUI table. An empty row is added to the table, the Telephony OUI, and the Description.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values

NOTE: All non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds.

3.14 GARP

The Generic Attribute Registration Protocol (GARP) provides a generic framework in which devices in a bridged LAN, e.g. end stations and switches, can register and de-register attribute values, such as VLAN Identifiers, with each other. In doing so, the attributes are propagated to devices in the bridged LAN, and these devices form a *reachability* tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines and variables for the registration and de-registration of attribute values. A GARP participation in a switch or an end station consists of a GARP application component, and a GARP Information Declaration (GID) component associated with each port of the switch. The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

3.14.1 Configuration

This page describes how to configure the basic GARP Configuration settings for all switch ports. The settings relate to the currently selected unit, as shown in the page header.

Web Interface

To configure GARP Port Configuration in the Web interface:

1. Click GARP Configure.
2. Specify GARP Configuration Parameters.
3. Click Save.

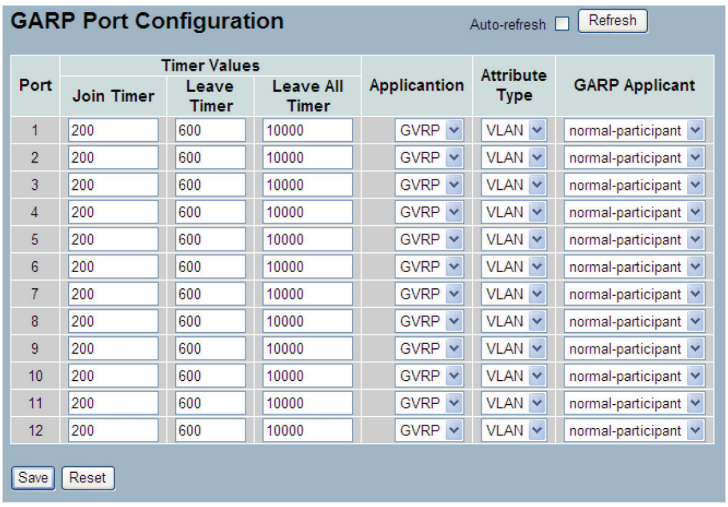


Figure 3-68. The GARP Port Configuration screen.

Parameter Description

- **Port**: The list of ports for which you can configure GARP settings. There are two types ofconfiguration settings that can be configured on a per-port basis.
  - Timer Values
  - Application
  - Attribute Type
  - GARP Applicant

- **Timer Values**: To set the GARP join timer, leave timer, and leave all timers, the unit is microseconds (ms).

  Three different timers can be configured on this page:

  - Join Timer: The default value for Join timer is 200 ms.

  - Leave Timer: The range of values for Leave Time is 600–1000 ms. The default value for Leave Timer is 600 ms.

  - Leave All Timer: The default value for Leave All Timer is 10000 ms.

- **Application**: Currently only supported application is GVRP.
- **Attribute Type**: Currently only supported Attribute Type is VLAN.
- **GARP Applicant**: This configuration is used to configure the Applicant state machine behavior for GARP on a particular port locally.

  - normal-participant: In this mode the Applicant state machine will operate normally in GARP protocol exchanges.

  - non-participant: In this mode the Applicant state machine will not participate in the protocol operation.

  The default configuration is normal participant.

- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values

3.14.2 Statistics

This section describes the port statistics of GARP for all switch ports. The port statistics relate to the currently selected unit, as shown in the page header.

Web Interface

To display GARP Port statistics in the Web interface:

1. Click GARP statistics.
2. Scroll to the port you want to display the GARP Counter information.
3. Click Refresh to modify the GARP statistics information.

Figure 3-69. The GARP Port Statistics screen.

Parameter Description

- **Port**: The Port column shows the list of all ports for which per-port GARP statistics are shown.
- **Peer MAC**: This is the MAC address of the neighboring switch from which the GARP frame is received.
- **Failed Count**: Records the quantity of all forwarding failure packets, which includes the failed forwarding attempts for Join and Leave messages.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the GARP Port Statistics information manually.

3.15 GVRP

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the function providing the VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP-state machines maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these information to other GVRP-aware devices to set up and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

3.15.1 Configuration

This page describes how to configure the basic GVRP Configuration settings for all switch ports. The settings relate to the currently selected unit, as shown in the page header.

Web Interface

To configure GVRP Port Configuration in the Web interface:

1. Click GVRP configure.
2. Specify GVRP Configuration Parameters.
3. Click Save.

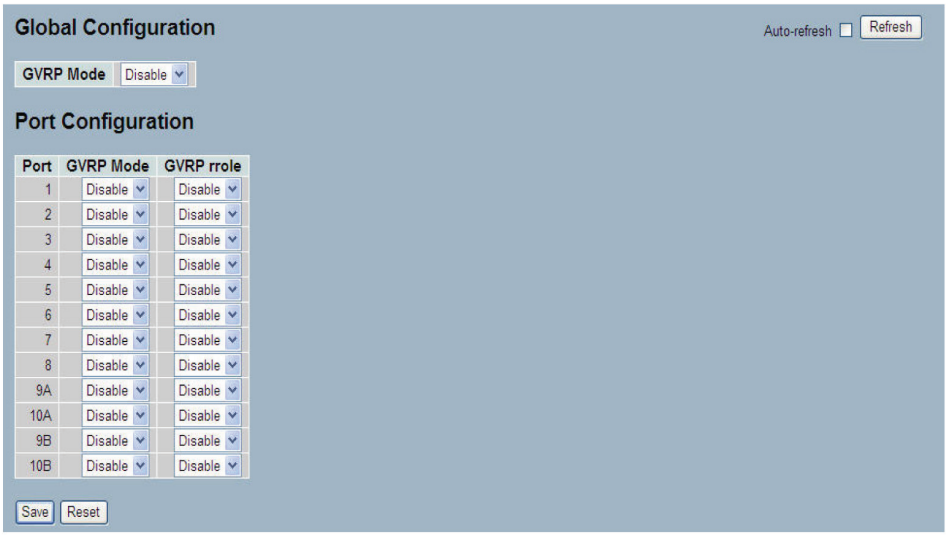


Figure 3-70. The GVRP Global Configuration.

Parameter Description

- **GVRP Mode**: GVRP Mode is a global setting, to enable the GVRP globally select 'Enable' from menu and to disable GVRP globally select "Disable."
- **Port**: The Port column shows the list of ports for which you can configure per port GVRP settings. There are two configuration settings which can be configured on per-port basis.
  - GVRP Mode
  - GVRP rrole

1. GVRP Mode

This configuration is to enable/disable GVRP Mode on particular port locally.

- Disable: Select to disable GVRP Mode on this port.

- Enable: Select to enable GVRP Mode on this port.

The default value of configuration is Disable.

2. GVRP role

This configuration is used to configure restricted role on an interface.

- Disable: Select to disable GVRP rrole on this port.

- Enable: Select to enable GVRP rrole on this port.

The default configuration is Disable.

- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the GVRP Global information manually.
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.15.2 Statistics

The section describes the basic GVRP Port statistics for all switch ports. The statistics relate to the currently selected unit, as shown in the page header.

Web Interface

To display GVRP Port statistics in the Web interface:

1. Click GVRP statistics.
2. Scroll to the port you want to display the GVRP Counter information.
3. Click Refresh to modify the GVRP statistics information.

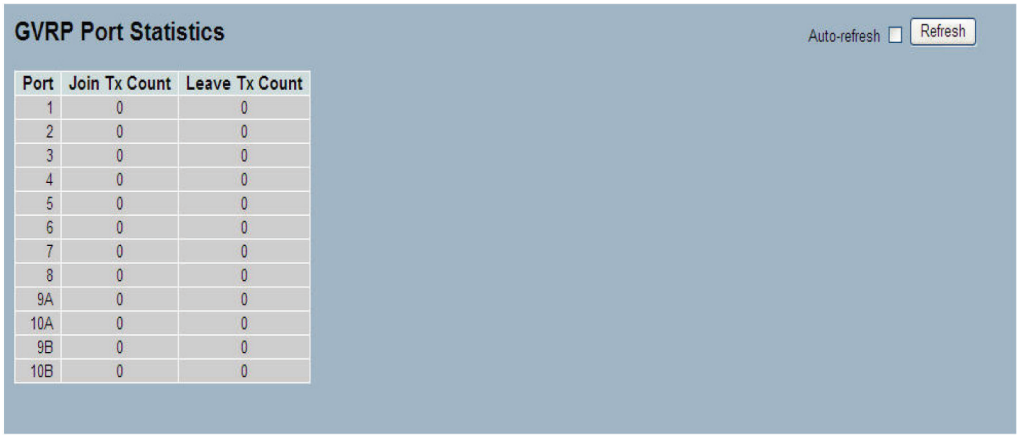


Figure 3-71. The GVRP Port Statistics screen.

Parameter Description

- **Port**: The Port column shows the list of ports for which you can see port counters and statistics.
- **Join Tx Count**: Records the number of Join message packets sent from the switch when GVRP is enabled and the VLAN is built up.
- **Leave Tx Count**: Records the number of Leave message packets sent from the switch when the VLAN group is cancelled.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the GVRP Port Statistics information manually.

3.16 QoS

The switch supports four QoS queues per port, with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

The switch supports advanced memory control mechanisms, providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. It also features a super priority queue with dedicated memory and the highest priority when instances of arbitration become necessary. The ingress super priority queue permits traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

3.16.1 Port Classification

This section describes how to configure the basic QoS Ingress Classification settings for all switch ports. The settings relate to the currently selected unit, as shown in the page header.

Web Interface

To configure the QoS Port Classification parameters in the Web interface:

1. Click Configuration, QoS, Port Classification.
2. Scroll to select QoS class, DP Level, PCP, and DEI parameters.
3. Click "Save" to save the setting.
4. To cancel the setting, click the Reset button to revert to previously saved values.

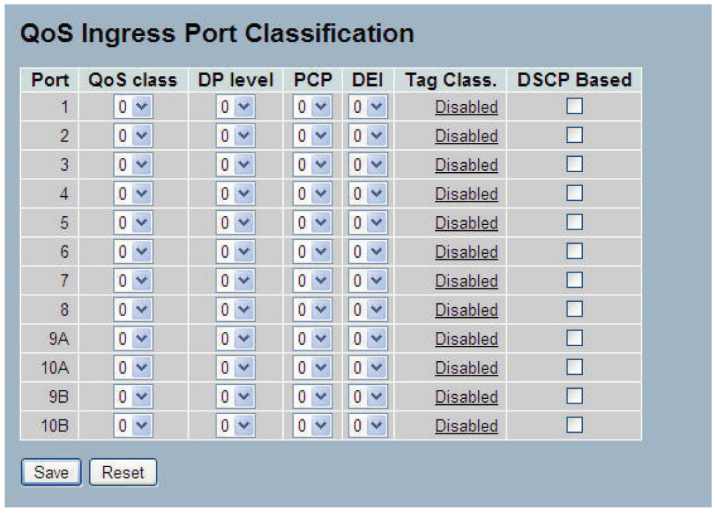


Figure 3-72. The QoS Configuration screen.

Parameter Description

- **Port**: The port number for which the configuration below applies.
- **QoS class**: Controls the default QoS class, i.e., the QoS class for frames not classified in any other way. There is a one-to-one mapping between QoS class, queue, and priority. A QoS class of 0 (zero) has the lowest priority.
- **DP level**: Controls the default DP level, i.e., the DP level for frames not classified in any other way.
- **PCP**: Controls the default PCP for untagged frames.
- **DEI**: Controls the default DEI for untagged frames.
- **Tag Class**: Shows the classification mode for tagged frames on this port.
  - Disabled: Use default QoS class and DP level for tagged frames.
  - Enabled: Use mapped versions of PCP and DEI for tagged frames.

  Click on the mode to configure the mode and/or mapping.
- **DSCP Based**: Click to enable DSCP Based QoS Ingress Port Classification.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.16.2 Port Policing

This section provides an overview of QoS Ingress Port Policers for all switch ports. Because voice and video usually maintain a steady rate of traffic, Port Policing is useful in constraining traffic flows and marking frames above specific rates.

Web Interface

To display the QoS Port Schedulers in the Web interface:

1. Click Configuration, QoS, Port Policing.
2. Select which port needs to enable the QoS Ingress Port Policers, and key in the Rate limit condition.
3. Scroll to select the Rate limit Unit with kbps, Mbps, fps and kfps.
4. Click Save to save the configuration.

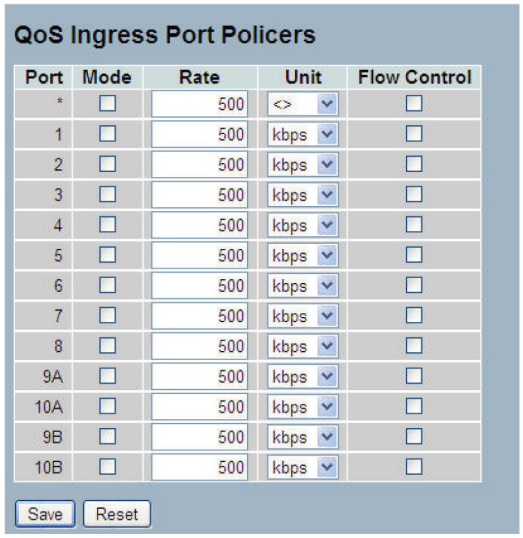


Figure 3-73. The QoS Ingress Port Policers Configuration screen.

Parameter Description

- **Port**: The logical port for the settings contained in the same row. Click on the port number to configure the schedulers.
- **Mode**: Check the port to enable the QoS Ingress Port Policers function.
- **Rate**: To set the rate limit value for this port, the default is 500.
- **Unit**: To scroll to select what unit of rate includes kbps, Mbps, fps and kfps. The default is kbps.
- **Flow Control**: To evoke to enable or disable flow control on port.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.16.3 Port Scheduler

This section provides an overview of QoS Egress Port Schedulers for all switch ports. and the ports belong to the currently selected unit, as stated in the screen header.

Web Interface

To display the QoS Port Schedulers in the Web interface:

1. Click Configuration, QoS, Port Schedulers.
2. Display the QoS Egress Port Schedulers.

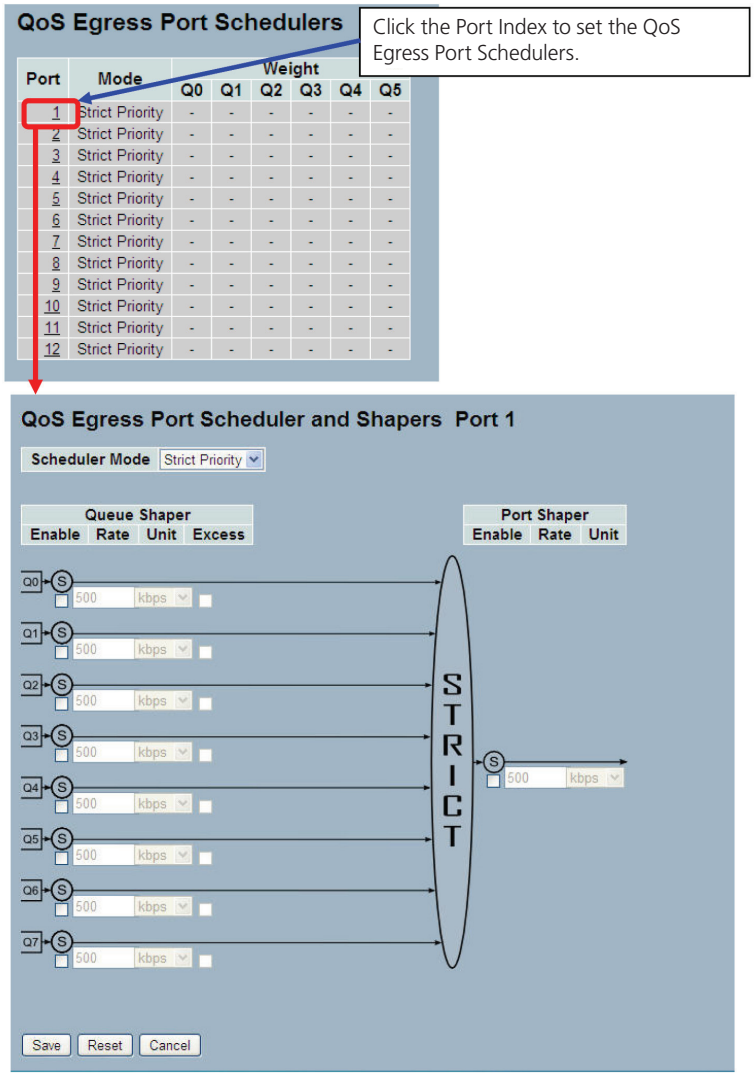


Figure 3-74. The QoS Egress Port Schedules front screen and Port Shapers screen in Strict Priority mode.

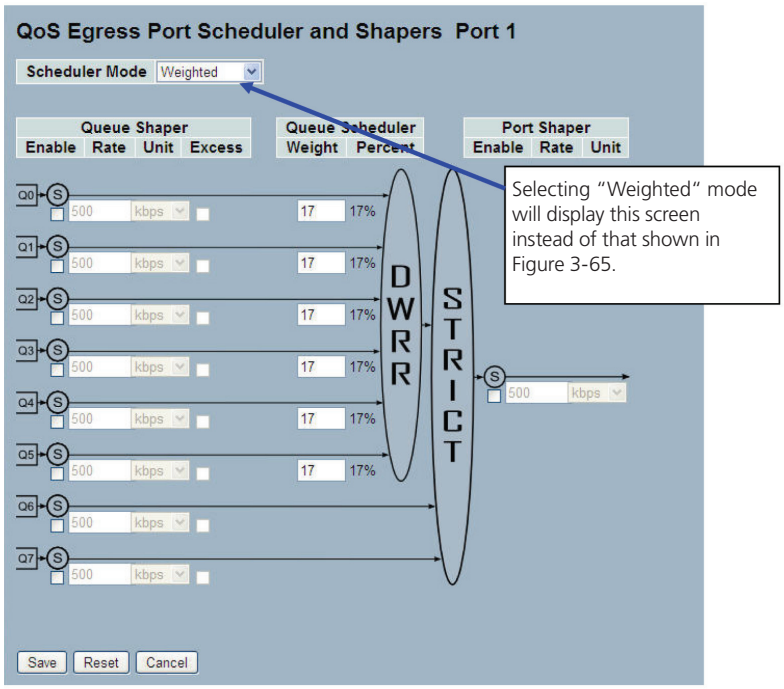


Figure 3-75. The QoS Egress Port Scheduler front screen in Weighted mode.

Parameter Description

- **Port**: The logical port for the settings contained in the same row. Click on the port number to configure the schedulers.
- **Mode**: Shows the scheduling mode for this port.
- **Weight (Qn)**: Shows the weight for this queue and port.
- **Scheduler Mode**: Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
- **Queue Shaper Enable**: Controls whether the queue shaper is enabled for this queue on this switch port.
- **Queue Shaper Rate**: Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100–1,000,000 when the "Unit" is "kbps", and it is restricted to 1–1000 when the "Unit" is "Mbps."
- **Queue Shaper Unit**: Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".
- **Queue Shaper Excess**: Controls whether the queue is allowed to use excess bandwidth.
- **Queue Scheduler Weight**: Controls the weight for this queue. The default value is "17." This value is restricted to 1–100. This parameter is only shown if "Scheduler Mode" is set to "Weighted."
- **Queue Scheduler Percent**: Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted."
- **Port Shaper Enable**: Controls whether the port shaper is enabled for this switch port.
- **Port Shaper Rate**: Controls the rate for the port shaper. The default value is 500. This value is restricted to 100–1,000,000 when the "Unit" is "kbps," and it is restricted to 1–1000 when the "Unit" is "Mbps."
- **Port Shaper Unit**: Controls the unit of measure for the port shaper rate as "kbps" or "Mbps." The default value is "kbps."
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.16.4 Port Shaping

This section provides an overview of QoS Egress Port Shaping for all switch ports. Others the user could get all detail information ot the ports belong to the currently selected unit, as shown in the page header.

Web Interface

To display the QoS Port Shapers screen in the Web interface:

1. Click Configuration, QoS, Port Shapers.
2. Display the QoS Egress Port Shapers.

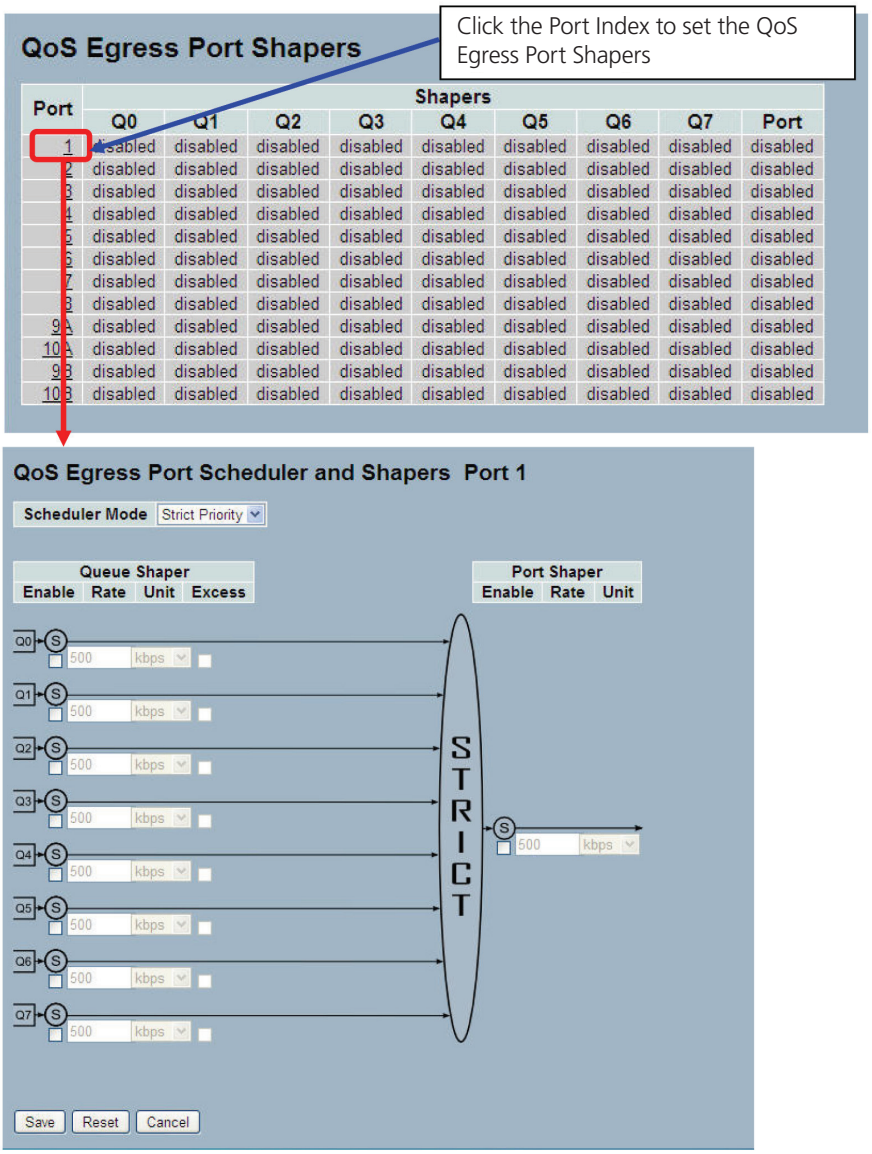


Figure 3-76. The QoS Egress Port Shapers screen, Strict Priority mode.

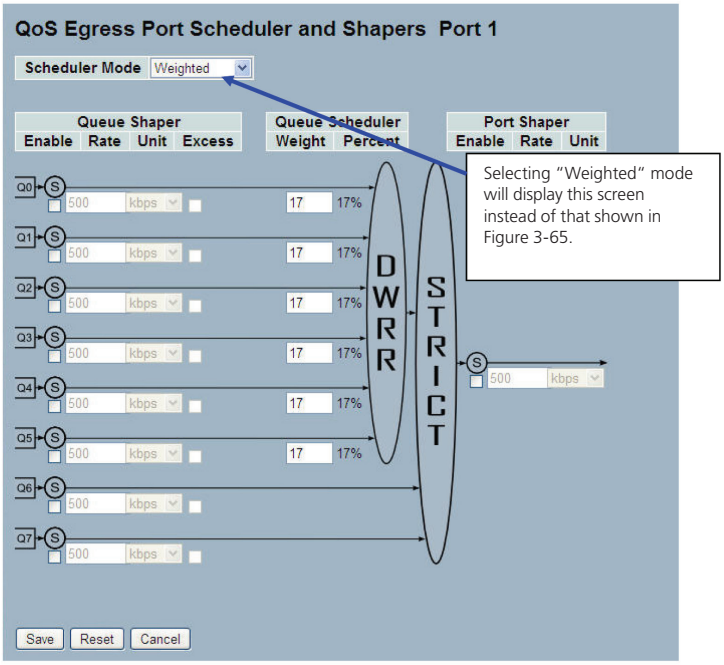


Figure 3-77. The QoS Egress Port Shapers screen, Weighted mode.

Parameter Description

- **Port**: The logical port for the settings contained in the row. Click on the port number to configure the shapers.
- **Shapers (Qn)**: Shows "disabled" or actual queue shaper rate, e.g. "800 Mbps."
- **Shapers (Port)**: Shows "disabled" or actual port shaper rate, e.g. "800 Mbps."
- **Scheduler Mode**: Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
- **Queue Shaper Enable**: Controls whether the queue shaper is enabled for this queue on this switch port.
- **Queue Shaper Rate**: Controls the rate for the queue shaper.
- **Queue Shaper Unit**: Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps." The default value is "kbps."
- **Queue Shaper Excess**: Controls whether the queue is allowed to use excess bandwidth.
- **Queue Scheduler Weight**: Controls the weight for this queue. The default value is "17." This value is restricted to 1–100. This parameter is only shown if "Scheduler Mode" is set to "Weighted."
- **Queue Scheduler Percent**: Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted."
- **Port Shaper Enable**: Controls whether the port shaper is enabled for this switch port.
- **Port Shaper Rate**: Controls the rate for the port shaper.
- **Port Shaper Unit**: Controls the unit of measure for the port shaper rate as "kbps" or "Mbps." The default value is "kbps."
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.16.5 Port Tag Remarking

This section provides an overview of QoS Egress Port Tag Remarking for all switch ports. Others the ports belong to the currently selected unit, as shown in the screen header.

Web Interface

To display the QoS Port Tag Remarking in the Web interface: Click Configuration, QoS, Port Tag Remarking.

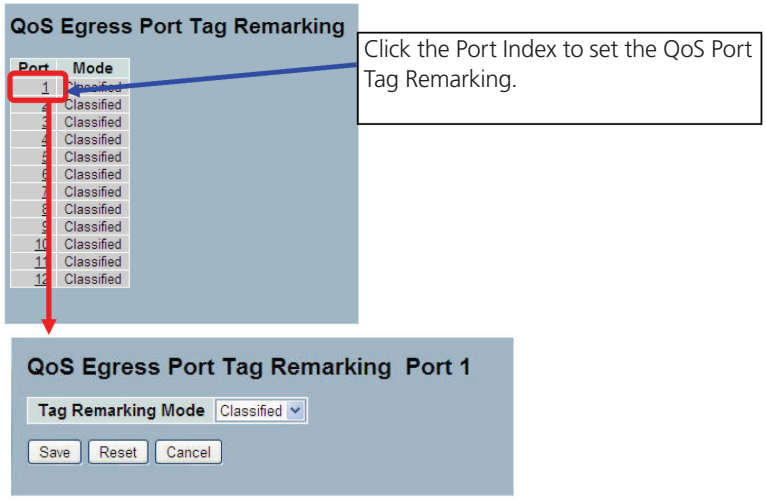


Figure 3-78. The Port Tag Remarking screen.

Parameter Description

- **Port**: The logical port for the settings contained in the same row. Click on the port number to configure tag remarking.
- **Mode**: Shows the tag remarking mode for this port.
  - Classified: Use classified PCP/DEI values.
  - Default: Use default PCP/DEI values.
  - Mapped: Use mapped versions of QoS class and DP level.
- **Tag Remarking Mode**: To scroll to select the tag remarking mode for this port.
  - Classified: Use classified PCP/DEI values.
  - Default: Use default PCP/DEI values.
  - Mapped: Use mapped versions of QoS class and DP level.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.
  - Cancel: Click to cancel the changes.

3.16.6 Port DSCP

The section describes how to set the QoS Port DSCP configuration, enabling you to configure the basic QoS Port DSCP Configuration settings for all switch ports. Others the settings relate to the currently selected unit, as shown in the page header.

Web Interface

To configure the QoS Port DSCP parameters in the Web interface:

1. Click Configuration, QoS, Port DSCP.
2. Evoke to enable or disable the Ingress Translate and Scroll the Classify Parameter configuration.
3. Scroll to select Egress Rewrite parameters.
4. Click the Save button to save the setting.
5. To cancel the setting, click the Reset button to revert to previously saved values.

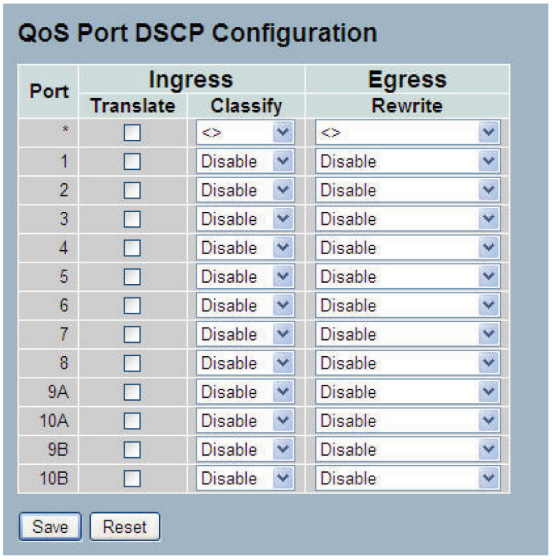


Figure 3-79. The QoS Port DSCP Configuration screen.

Parameter Description

- **Port**: The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.
- **Ingress**: In Ingress settings you can change ingress translation and classification settings for individual ports.

  There are two configuration parameters available in Ingress:

  1. Translate: To Enable the Ingress Translation, click the checkbox.
  2. Classify: Classifications for a port have four different values.:

  - Disable: No Ingress DSCP Classification.
  - DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.
  - Selected: Classify only the selected DSCP for which classification is enabled as specified in the DSCP Translation window for the specific DSCP.
  - All: Classify all DSCP.

- Egress: Port Egress Rewriting can be one of these parameters:
  - Disable: No Egress rewrite.
  - Enable: Rewrite enable without remapped.
  - Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.
- Buttons:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.16.7 DSCP-Based QoS

This section describes how to configure the DSCP-Based QoS mode for the basic DSCP-based QoS Ingress Classification settings for all switches.

Web Interface

To configure the DSCP-Based QoS Ingress Classification parameters in the Web interface:

1. Click Configuration, QoS, DSCP-Based QoS.
2. Enable or disable the DSCP for Trust.
3. Scroll to select QoS Class and DPL parameters.
4. Click the Save button to save the setting.
5. To cancel the setting, click the Reset button to revert to previously saved values.

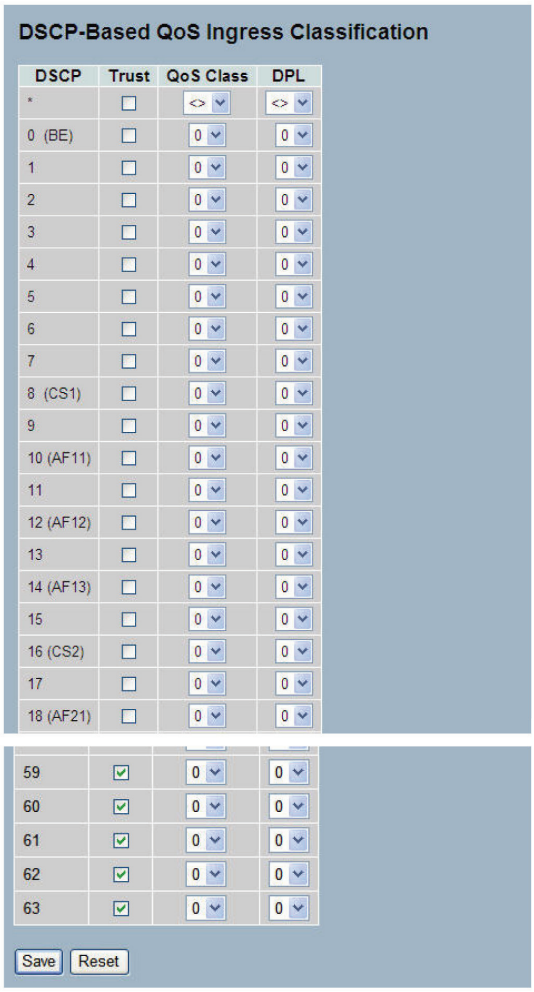


Figure 3-80. The DSCP-Based QoS Ingress Classification Configuration screen.

Parameter Description

- **DSCP**: Maximum number of supported DSCP values are 64.
- **Trust**: Click to check if the DSCP value is trusted.
- **QoS Class**: QoS Class value can be any of (0-7).
- **DPL**: Drop Precedence Level (0-3).
- Buttons:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.16.8 DSCP Translation

This section describes how you can configure the basic QoS DSCP Translation settings for all switches. DSCP Translation can be done in Ingress or Egress.

Web Interface

To configure the DSCP Translation parameters in the Web interface:

1. Click Configuration, QoS, DSCP Translation.
2. Scroll to set the Ingress Translate and Egress Remap DP0 and Remap DP1 Parameters.
3. Evoke to enable or disable Classify.
4. Click the Save button to save the setting.
5. To cancel the setting, click the Reset button to revert to previously saved values.

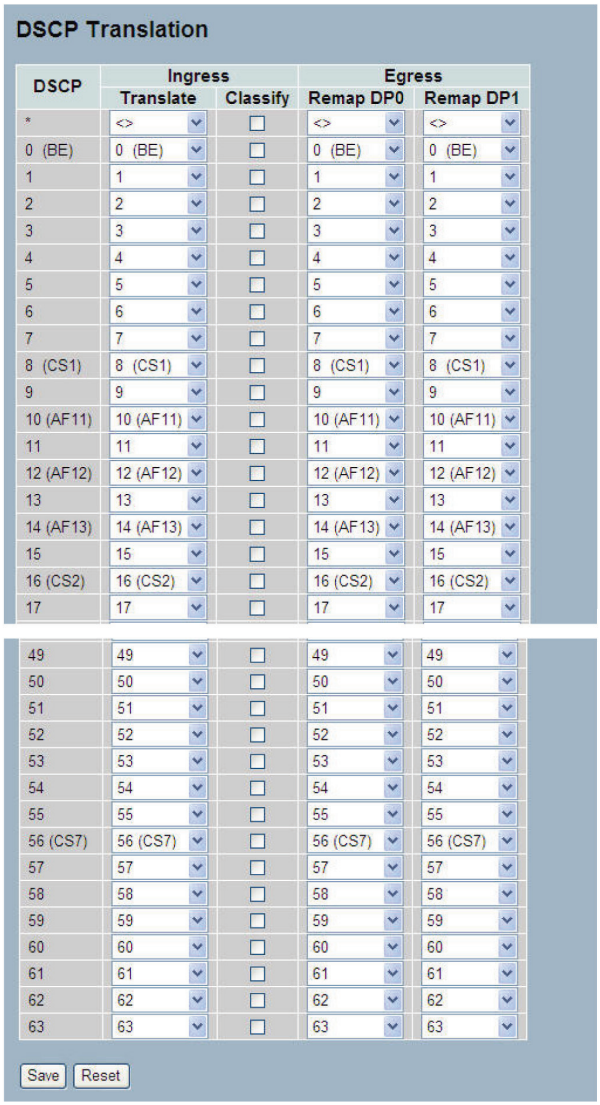


Figure 3-81. The DSCP Translation Configuration screen

Parameter Description

- **DSCP**: Maximum number of supported DSCP values are 64, and valid DSCP value ranges from 0 to 63.
- **Ingress**: The Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP translation:

  1. Translate : DSCP at Ingress side can be translated to any of (0–63) DSCP values.

  2. Classify : Click to enable Classification at Ingress side.

- **Egress**: The following configurable parameters are for the Egress side:

  1. Remap DP0 : Select the DSCP value from select menu to which you want to remap. DSCP values range from 0 to 63

  2. Remap DP1 : Select the DSCP value from select menu to which you want to remap. DSCP values range from 0 to 63.

  Following this, there is a configurable parameter for the Egress side.

  Remap: Select the DSCP value from select menu to which you want to remap. DSCP values range from 0 to 63.

- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.16.9 DSCP Classification

This section describes how to configure and map DSCP value to a QoS Class and DPL value. Others the settings relate to the currently selected unit, as shown in the page header.

Web Interface

To configure the DSCP Classification parameters in the Web interface:

1. Click Configuration, QoS, DSCP Translation.
2. Scroll to set the DSCP Parameters.
3. Click the Save button to save the setting.
4. To cancel the setting, click the Reset button to revert to previously saved values.

Figure 3-82. The DSCP Classification Configuration screen.

Parameter Description

- **QoS Class**: Available QoS Class value ranges from 0 to 7. QoS Class (0–7) can be mapped to following parameters.
- **DPL**: Drop Precedence Level (0–1) can be configured for all available QoS Classes.
- **DSCP**: Select DSCP value (0–63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.16.10 QoS Control List Configuration

This section shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

Web Interface

To configure the QoS Control List parameters in the Web interface:

1. Click Configuration, QoS, QoS Contol List.
2. Click the ⊕ to add a new QoS Control List.
3. Scroll all parameters and evoke the Port Member to join the QCE rules.
4. Click the Save button to save the setting.
5. To cancel the setting, click the Reset button to revert to previously saved values.

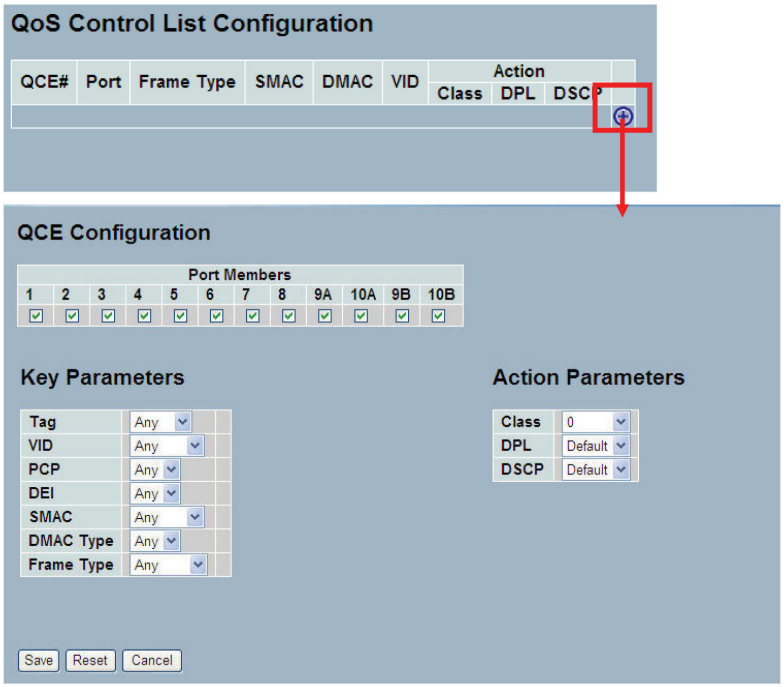


Figure 3-83. The QoS Control List Configuration screen.

Parameter Description

- **QCE#**: Indicates the index of QCE.
- **Port**: Indicates the list of ports configured with the QCE.
- **Frame Type**: Indicates the type of frame to look for incoming frames. Possible frame types are:

  Any: The QCE will match all frame types.

  Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

  LLC: Only (LLC) frames are allowed.

  SNAP: Only (SNAP) frames are allowed

  IPv4: The QCE will match only IPV4 frames.

  IPv6: The QCE will match only IPV6 frames.

- **SMAC**: Displays the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.
- **DMAC**: Specify the type of Destination MAC addresses for incoming frame. Possible values are:

  Any: All types of Destination MAC addresses are allowed.

  Unicast: Only Unicast MAC addresses are allowed.

  Multicast: Only Multicast MAC addresses are allowed.

  Broadcast: Only Broadcast MAC addresses are allowedd.

  The default value is "Any."

- **VID**: Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range of 1 to 4095, or "Any."
- **Conflict**: Displays QoS Control Entry (QCE) status. It may happen that resources required to add a QCE may not available, in that case it shows conflict status as "Yes." Otherwise it is always "No."

NOTE: This conflict can be resolved by releasing the resource required by the QCE and pressing the Refresh button.

- **Action**: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

  There are three action fields: Class, DPL, and DSCP:

  Class: Classified QoS Class; if a frame matches the QCE, it will be put in the queue.

  DPL: Drop Precedence Level; if a frame matches the QCE, then the DP level will set to value displayed under DPL column.

  DSCP: If a frame matches the QCE, then DSCP will be classified with the value displayed under DSCP column.

- **Modification Buttons**: You can modify each QCE in the table using the following buttons:

  : Inserts a new QCE before the current row.

  : Edits the QCE.

  : Moves the QCE up the list.

  : Moves the QCE down the list.

  : Deletes the QCE.

  : The lowest plus sign adds a new entry at the bottom of the QCE listings.
- **Port Members**: Check the checkbox button to make any port member of the QCL entry. By default all ports will be checked.
- **Key Parameters**: Key configuration are discribed as below:

  Tag Value of Tag field can be 'Any', 'Untag' or 'Tag'

  VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

  PCP Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0–1, 2–3, 4–5, 6–7, 0–3, 4–7) or 'Any.'

  DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any.'

  SMAC Source MAC address: 24 MS bits (OUI) or 'Any.'

DMAC Type Destination MAC type: possible values are unicast (UC), multicast (MC), broadcast (BC) or 'Any.'

Frame Type can have any of the following values:

1. Any
2. Ethernet
3. LLC
4. SNAP
5. IPv4
6. IPv6

All frame types are explained below:

1. Any: Allow all types of frames.
2. Ethernet: A valid Ethernet type can have a value within 0x600-0xFFFF or 'Any.' The default value is 'Any.'
3. LLC: A valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'. The default value is 'Any'. A valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'. The default value is 'Any'. A valid Control Address can vary from 0x00 to 0xFF or 'Any'. The default value is 'Any.'
4. SNAP : A valid PID (a.k.a ethernet type) can have value within 0x00-0xFFFF or 'Any.' The default value is 'Any.'
5. IPv4 : A valid protocol IP may range from 0–255 (TCP or UDP) or 'Any'. A specific Source IP address in the value/mask format or 'Any'. The IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.

   DSCP Diffserv Code Point value (DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0–63 including BE, CS1–CS7, EF or AF11–AF43 IP Fragment IPv4 frame fragmented option: yes|no|any Sport Source TCP/UDP port: (0–65535) or 'Any.' A specific or port range applicable for IP protocol UDP/TCP Dport Destination TCP/UDP port: (0–65535) or 'Any.' A specific or port range applicable for IP protocol UDP/TCP.
6. IPv6 :Protocol IP protocol number: (0–255, TCP or UDP) or 'Any' Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits DSCP Diffserv Code Point value (DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0–63 including BE, CS1–CS7, EF or AF11–AF43.

   Sport Source TCP/UDP port: (0–65535) or 'Any,' specific or port range applicable for IP protocol UDP/TCP Dport Destination TCP/UDP port: (0–65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

- Action Configuration:

  Class QoS Class: class (0–7), default- basic classification.

  DP Valid DP Level can be (0–3), default- basic classification.

  DSCP Valid dscp value can be (0–63, BE, CS1–CS7, EF or AF11–AF43).

- Buttons:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.16.11 QCL Status

This section describes how to configure the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware because of hardware limitations. The maximum number of QCEs is 256 on each switch.

Web Interface

To display the QoS Control List Status in the Web interface:

1. Click Configuration, QoS , QCL Status.
2. To Auto-refresn information, check "Auto-refresh".
3. Scroll to select the combined, static, Voice VLAN and conflict.
4. Click "Refresh" to refresh an entry of the MVR Statistics Information.

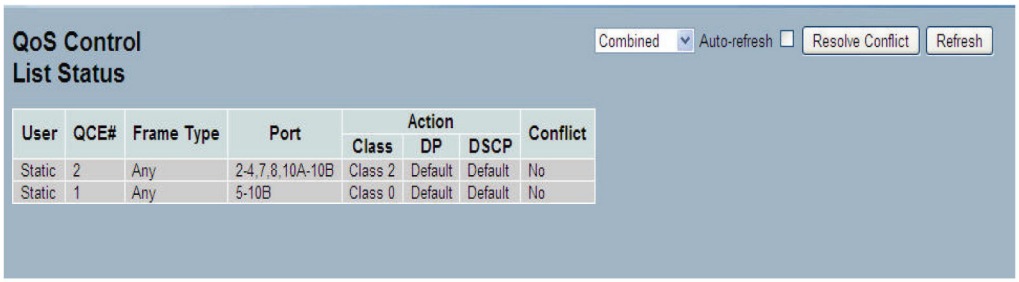


Figure 3-84. The QoS Control List Status screen.

Parameter Description

- **User**: Indicates the QCL user.
- **QCE#**: Indicates the index of QCE.
- **Frame Type**: Indicates the type of frame to search for incoming frames. Possible frame types are:

  Any: The QCE will match all frame type.

  Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

  LLC: Only (LLC) frames are allowed

  LLC: Only (SNAP) frames are allowed.

  IPv4: The QCE will match only IPV4 frames.

  IPv6: The QCE will match only IPV6 frames.
- **Port**: Indicates the list of ports configured with the QCE.
- **Action**: Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP:

  Class: Classified QoS Class; if a frame matches the QCE it will be put in the queue.

  DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.

  DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.
- **Conflict**: Displays QCE status. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes.' Otherwise it is always 'No.'

NOTE: Conflict can be resolved by releasing the resource required by the QCE and pressing the Refresh button.

- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Resolve Conflict**: Click it to resolve confict issues.
- **Icon, upper right of screen (Refresh)**: Click to refresh the QCL information manually.

3.16.12 Storm Control

This section describes how to configure the Storm control for the switch. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch

Web Interface

To configure the Storm Control Configuration parameters in the Web interface:

1. Click Configuration, QoS, Storm Control Configuration.
2. Select the frame type to enable storm control.
3. Scroll to set the Rate Parameters.
4. Click the Save button to save the setting.
5. Click the Reset button to cancel and revert to previously saved values.

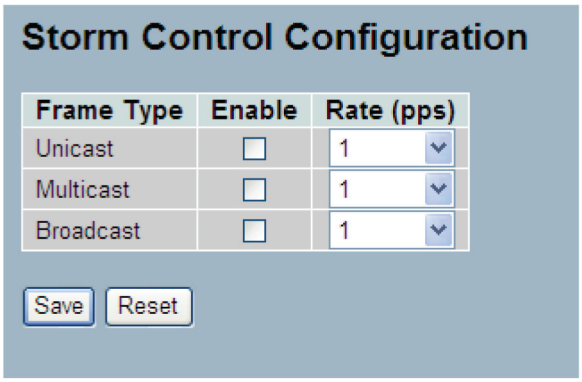


Figure 3-85. The Storm Control Configuration screen.

Parameter Description

- **Frame Type**: The settings in a particular row apply to the frame type listed here: Unicast, Multicast, or Broadcast.
- **Enable**: Enable or disable the storm control status for the given frame type.
- **Rate**: The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, 1024K, 2048K, 4096K, 8192K, 16384K, or 32768K. The 1 kpps is actually 1002.1 pps.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.17 Thermal Protection

This section describes how to inspect and configure current settings for controlling thermal protection. Thermal protection is used to protect the chip from becoming overheated.

3.17.1 Configuration

When the temperature exceeds the configured thermal protection temperature, ports will be turned off to decrease the power consumption. It is possible to arrange the ports with different priorities. Each priority can be given a temperature at which the corresponding ports will be turned off.

Web Interface

To configure the Thermal Protection in the Web interface:

1.Click Configuration, Thermal Protection, Configuration.

2. Specify the temperature in the priority 0 to 3.

3. Scroll to set the Priority.

4. Click the Save button to save the setting.

5. To cancel the setting, click the Reset button to revert to previously saved values.

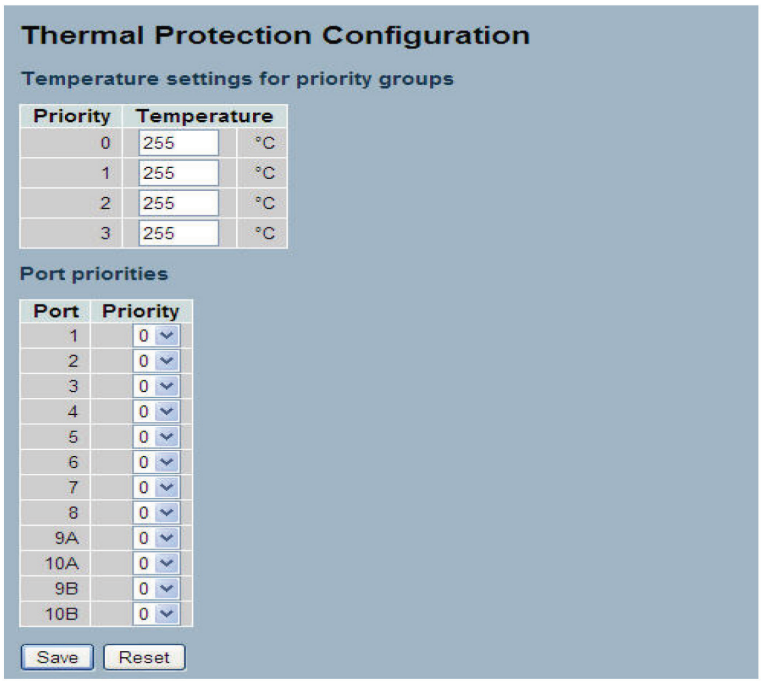


Figure 3-86. The Thermal Protection Configuration screen.

Parameter Description

Temperature settings for priority groups

The temperature at which the ports with the corresponding priority will be turned off.

- **Priority**: The criteria index for thermal protect trigger temperature, indexed from 0 to 3.
- **Temperature**: To set the temperature criterion to trigger the thermal protect.

NOTE: The temperature means the MAC and PHY chipset's TA temperature, not the PSU device or environment temperature. Do not set environment temperature limitation value.

- **Port priorities**: This indicates the priority for each port. It allows the user to set what priority criterion is used to trigger the Port to be turned off via thermal protection.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.17.2 Status

The section allows the user to inspect the thermal status information related to thermal protection when users configure the Thermal protection function already.

Web Interface

To display the Thermal Protection Status in the Web interface: Click Configuration, Thermal Protection, Status.

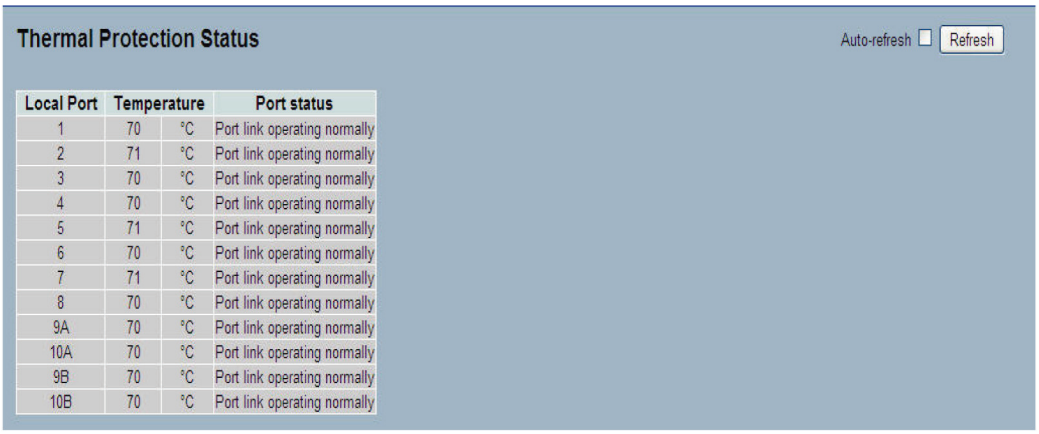


Figure 3-87. The Thermal Protection Status screen.

Parameter Description

- **Local Port**: Indicates the list of physical ports.
- **Temperature**: Shows the current chip temperature in degrees Celsius.

NOTE: The temperature means the MAC and PHY chipset's TA temperature, not the PSU device temperature or the environment temperature.

- **Port Status**: Displays the port status (includes link up or link down).
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the Port Current Temperature information manually.

3.18 sFlow Agent

The sFlow Collector configuration for the switch can be monitored and modified here. Up to one Collector is supported. This section contains instructions on how to configure sFlow collector IP type, sFlow collector IP Address, and Port Number for each sFlow Collector.

3.18.1 sFlow Collector

The "Current" field displays the currently configured sFlow Collector. The "Configured" field displays the new Collector Configuration.

Web Interface

To configure the sFlow Agent in the Web interface:

1. Click Configuration, sFlow Agent, Collector.
2. Set the parameters.
3. Scroll to IP Type to choose IPv4 or IPv6.
4. Click Save to save.
5. To cancel, click the Reset button to revert to previously saved values.

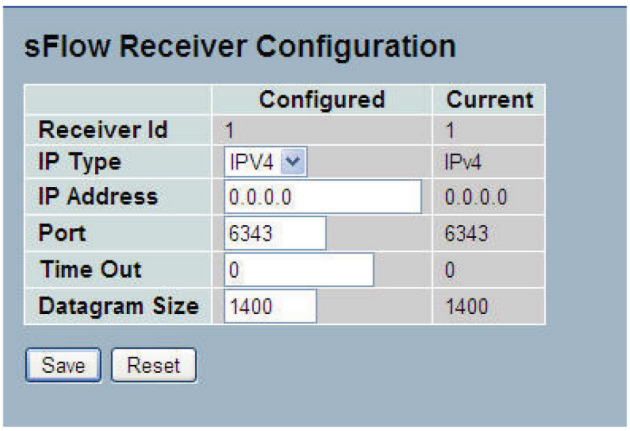


Figure 3-88. The sFlow Collector Configuration screen.

Parameter Description

- **Receiver ID**: The "Receiver ID" input fields allow the user to select the receiver ID. Indicates the ID of this particular sFlow Receiver. Currently one ID is supported as one collector is supported.
- **IP Type**: A dropdown list to select the type of IP of Collector is displayed. By default, IPv4 is the Collector IP type. Works using IPv4 or IPv6.
- **IP Address**: The address of a reachable IP is to be entered into the text box.

  This IP is used to monitor the sFlow samples sent by sFlow Agent (our switch).

  By default, The IP is set to 0.0.0.0, and a new entry has to be added to it.
- **Port**: A port to listen to the sFlow Agent has to be configured for the Collector. The value of the port number has to be typed into the text box. The value accepted is within the range of 1–65535. But an appropriate port number not used by other protocols need to be configured. By default, the port's number is 6343.

- **Time out**: It is the duration during which the collector receives samples, Once it is expired, the sampler stops sending the samples. It is through the management the value is set before it expires. The value accepted is within the range of 0-2147483647. By default it is set to 0.
- **Datagram Size**: The maximum UDP datagram size to send out the sFlow samples to the receiver. The value accepted is within the range of 200-1500 bytes. The default is 1400 bytes.
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.18.2 Sampler

This section displays the sFlow sampler and how to edit it. This will help the user based on a defined sampling rate, an average of 1 out of N packets/operations is randomly sampled. This type of sampling does not provide a 100% accurate result, but it does provide a result with quantifiable accuracy.

Web Interface

To configure the sFlow Agent in the Web interface:

1. Click Configuration, sFlow Agent, sampler.
2. Click the ⓔ to edit the sFlow sampler parameters.
3. Scroll to Sample Type to choice with None, Tx, Rx or All.
4. Click Save to save the setting.
5. Click the Reset button to cancel and revert to previously saved values.

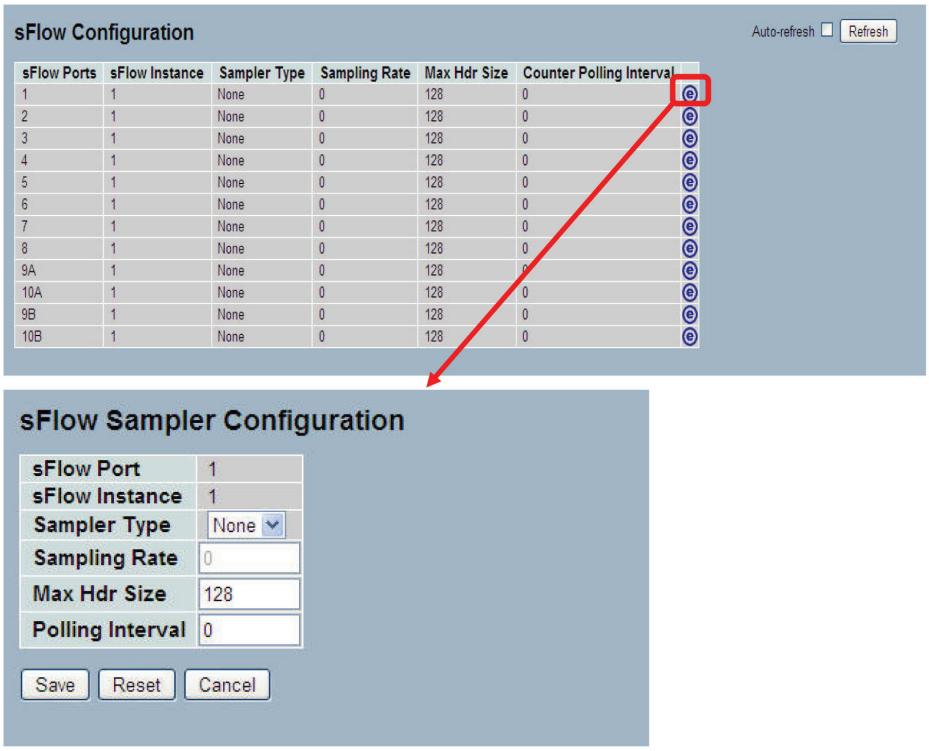


Figure 3-89. The sFlow Sampler Configuration screen.

Parameter Description

- **sFlow Ports**: List of the port numbers on which sFlow is configured.
- **sFlow Instance**: Configured sFlow instance for the port number.
- **Sampler Type**: Configured sampler type on the port and could be any of the types: None, Rx, Tx or All. Scroll to choose. By default, The value is "None".
- **Sampling Rate**: Configured sampling rate on the ports.
- **Max Hdr Size**: Configured size of the header of the sampled frame.
- **Polling Interval**: Configured polling interval for the counter sampling.
- **Buttons**:
  - Edits the Data source sampler configuration.
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.
  - Cancel: Click to clear any unsaved changes you have made.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the sFlow Sampler information manually.

3.19 Loop Protection

Loop protection detects the presence of traffic. When a switch becomes aware that a packet's (looping protection frame) MAC address is the same as that of its own port, loop protection activates. The port will be locked when it receives the looping protection frames. To resume the locked port, locate and remove the looping path, select the locked port, and click on "Resume."

3.19.1 Configuration

To set loop protection:

Web Interface

To configure the loop protection parameters in the Web interface:

1. Click "Configuration, loop protection, Configuration."
2. Click to select enable or disable the port loop protection.
5. Click "Save" to save the setting.
6. Click the Reset button to cancel and revert to previously saved values.

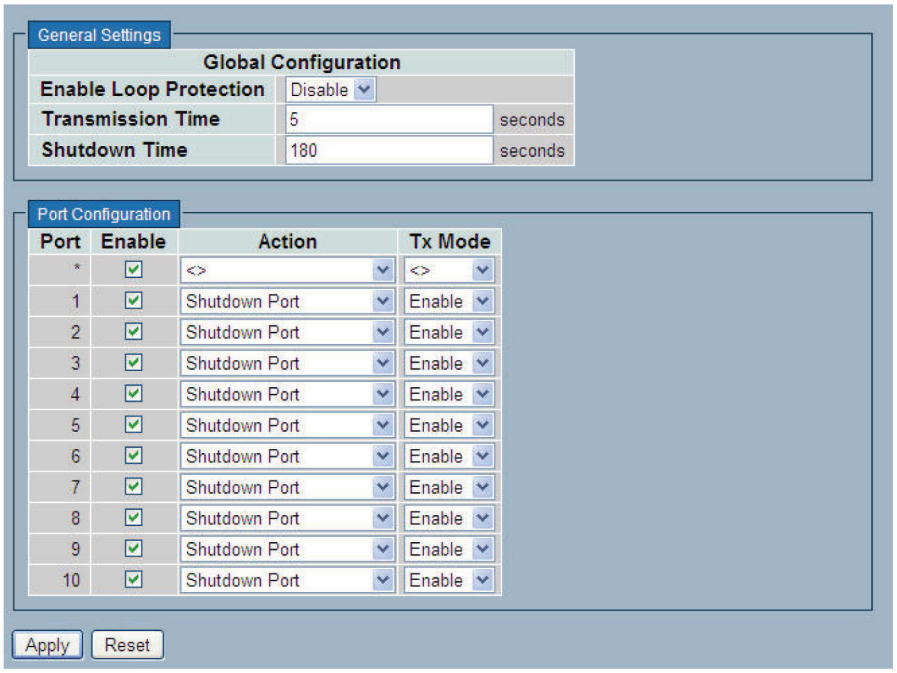


Figure 3-90. The Loop Protection Configuration screen.

Parameter Description

- **Enable Loop Protection**: Controls whether loop protection is enabled (as a whole).
- **Transmission Time**: The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.
- **Shutdown Time**: The period (in seconds) for which a port will be kept disabled if a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).
- **Port No**: The switch port number of the port.
- **Enable**: Controls whether loop protection is enabled on this switch port.

- **Action**: Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.
- **Tx Mode**: Controls whether the port is actively generating loop protection PDUs, or whether it is just passively looking for looped PDUs.
- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

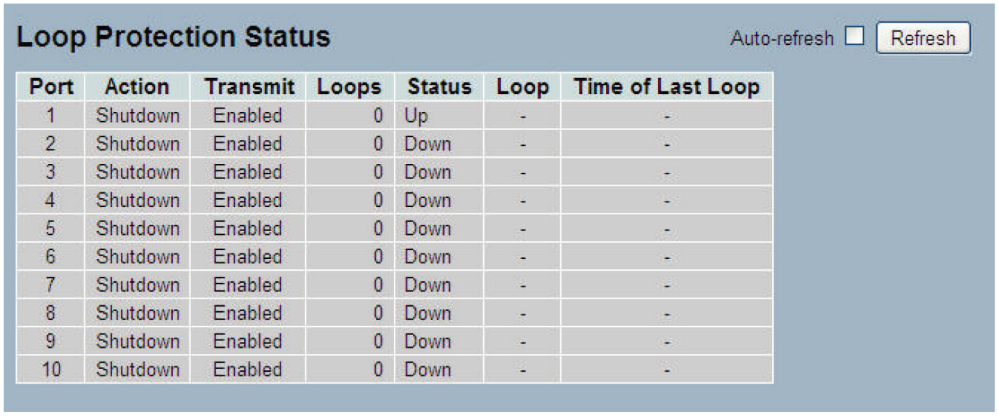
3.19.2 Status

This section describes how to display the loop protection status.

Web Interface

To display the loop protection parameters in the Web interface:

1. Click Configuration, Loop Protection, Status.
2. Check the box to enable or disable the auto-refresh.
3. Click "Refresh" to clear or update the record of loop protection.



Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-

Figure 3-91. The Loop Protection Status screen.

Parameter Description

- **Port**: The switch port number of the logical port.
- **Action**: The currently configured port action.
- **Transmit**: The currently configured port transmit mode.
- **Loops**: The number of loops detected on this port.
- **Status**: The current loop protection status of the port.
- **Loop**: Whether a loop is currently detected on the port.
- **Time of Last Loop**: The time of the last loop event detected.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the Loop Protection status information manually.

3.20 Single IP

Single IP Management (SIM) is a simple and useful method to optimize network utilities and management, designed to manage a group of switches as a single entity, called a SIM group. The SIM feature will enable users to:

- Simplify management of small workgroups or wiring closets while scaling networks to handle increased bandwidth demand.
- Reduce the number of IP addresses needed on the network.
- Virtual stacking structure—Eliminate any specialized cables for stacking and remove the distance barriers that typically limit topology options when using other stacking technology.

Web Interface

To configure the Single IP in the Web interface:

1. Click Configuration, Single IP.
2. Set the parameters.
3. Scroll to Role for to set the mode on the Single IP with Disabled, Master, Slave.
4. Click the Save button to save the setting
5. Click Reset to undo any changes made locally and revert to previously saved values.

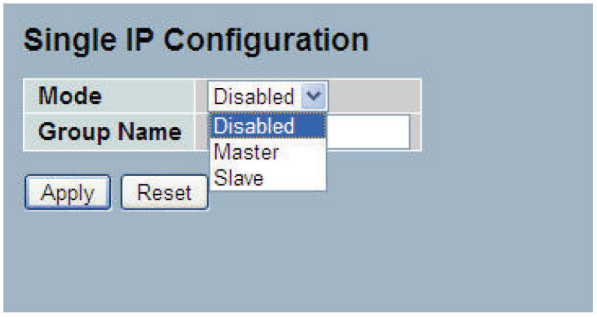


Figure 3-92. The Single IP Configuration screen.

Parameter Description

- **Mode**: Disable the SIP function, or set the device to a Master or Slave role.
- **Group name**: Set a group name when you create a Single IP management Group, up to 64 characters.
  - Master: The role is root. User connects to the Master and can control the Slaves in the same SIP group.
  - Slave: The role is slave. User connects to the switch what is a slave via Mastermanagement GUI.
- **Buttons**:
  - Apply: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

Web Interface

To show the Single IP in the Web interface:

1. Click Configuration, Single IP, and then Information.
2. Click refresh, or check auto-refresh to automaticaly update Information.

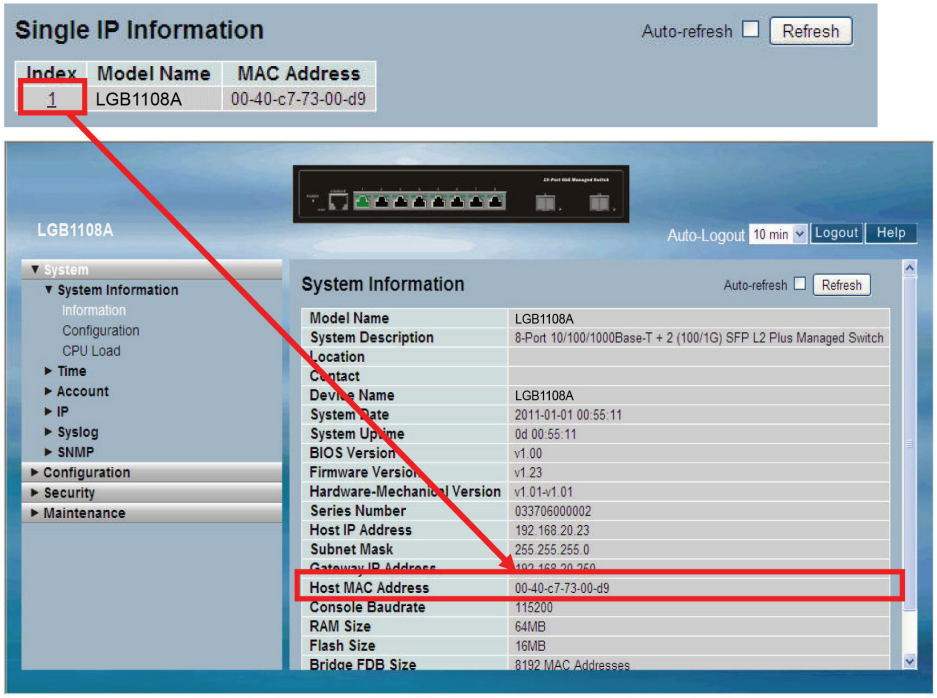


Figure 3-93. The Single IP Information screen.

Parameter Description

- **Index**: Indicates how many slave devices connect to the SIP group.
- **Model name**: Indicates what kind device has joined this SIP group.
- **MAC Address**: The parameter lets you to know what device's MAC address and join to this SIP group.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the LLDP Neighbors information manually.

NOTE: Click Index to redirect to the slave device and manually configure the display/management of the device.

3.21 Easy Port

Easy Port provides a convenient way to save and share common configurations. Use it to enable features and settings based on the location of a switch in the network and for mass configuration deployments across the network, including Voice IP phones, wireless access points and IP cameras, Or leverage it to run a converged voice, video, and data network considering quality of service (QoS), bandwidth, latency, and high performance.

Web Interface

To configure the Easy Port in the Web interface:

1. Click Configuration, Easy Port.
2. Set the parameters.
3. Scroll to Role for the kind device you are connecting.
4. Click Save to save the setting.
5. Click the Reset button to undo any changes made locally and revert to previously saved values.

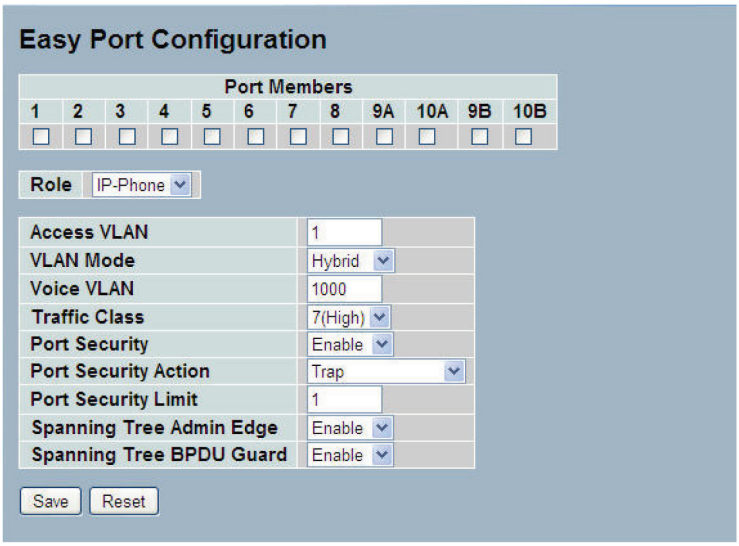


Figure 3-94. The Easy Port Configuration screen.

Parameter Description

- **Port Members**: Set the ports where the Easy Port function is enabled.
- **Role**: Select the kind of device to connect.
- **Access VLAN**: Set the switch port access VLAN ID (AVID).
- **VLAN Mode**: Select the VLAN mode with Access, Trunk, or Hybrid.
- **Voice VLAN**: Assign the Voice VLAN ID by entering the value of the port number.
- **Traffic Class**: Select the traffic class for the data stream priority. The available value from 0 (Low) to 7 (High). To assign a high priority, set the value to 7.
- **Port Security**: Enable or disable the Port Security function. If you turn on the function, set Port Security limit to allow how many devices can access the port (via MAC address).
- **Port Security Action**: Select from the pull-down menu to set which times the device isn't permitted to access the switch action: as trap, shutdown, or trap and shutdown.

- **Port Security limit**: Set the Port security limit here. The default is 1.
- **Spanning Tree Admin Edge**: Enable or disable the Spanning Tree Admin Edge function.
- **Spanning Tree BPDU Guard**: Enable or disable the Spanning Tree BPDU Guard function on the Easy Port.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.22 Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. The Mirror Configuration enables you to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

Web Interface

To configure the Mirror in the Web interface:

1. Click Configuration, Mirroring.
2. Scroll to select "Port to mirror on" for the port you'd like to select.
3. Scroll to disabled, enable, TX Only, and RX Only to set the Port Mirror mode.
4. Click Save to save the setting.
5. Click Revert to undo any changes made locally and revert to previously saved values.

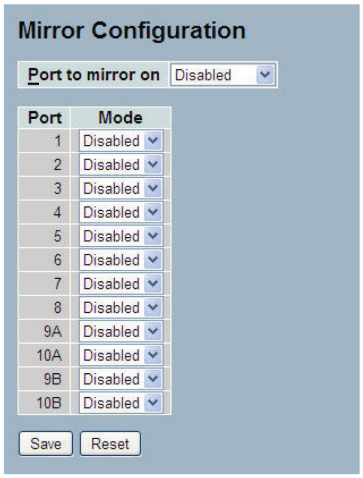


Figure 3-95. The Mirror Configuration screen.

Parameter Description

- **Port to mirror on**: Port to mirror also known as the mirror port. Frames from ports that have either source (Rx) or destination (Tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

Mirror Port Configuration: The following are used for Rx and Tx enabling.

- **Port**: The logical port for the settings contained in the same row.
- **Mode**: Select mirror mode:
  - Rx only Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.
  - Tx only Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.
  - Disabled: Neither frames transmitted nor frames received are mirrored.
  - Enabled: Frames received and frames transmitted are mirrored on the mirror port.

NOTE: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

- **Buttons**: Click "Save" to save changes, or "Reset" to undo any changes made locally and revert to previously saved values.

3.23 Trap Event Severity

This function is used to set a Alarm trap and get the Event log. The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events occurred.

Web Interface

To configure the Trap Event Severity Configuration in the Web interface:

1. Click Configuration, Trap Event Severity Configuration.
2. Scroll to select the Group name and Severity Level.
3. Click Save to save the setting.
4. To cancel any changes before saving, click the Reset button to revert to previously saved values.

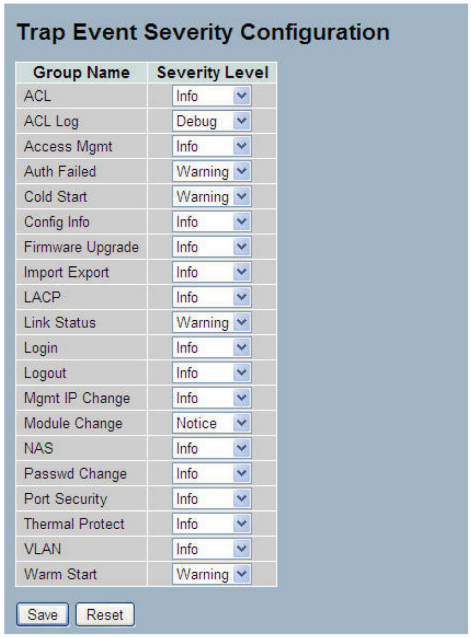


Figure 3-96. The Trap Event Severity Configuration screen.

Parameter Description

- Group Name: The field describes the Trap Event definition.
- Severity Level: Select the event type with "Emerg", "Alert", "Crit", "Error", "Warming", "Notice", "Info" and "Debug".
- Buttons:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.24 SMTP Configuration

When the switch perceives an alarm, use this function to enable the SMTP server to send you an alarm e-mail.

Web Interface

To configure the SMTP Configuration in the Web interface:

1. Click Configuration, SMTP Configuration.
2. Scroll to select the Severity Level.
3. Specify the parameters in each blank field.
4. Click the Save button to save the setting.
5. Click Reset to undo any changes made locally and revert to previously saved values

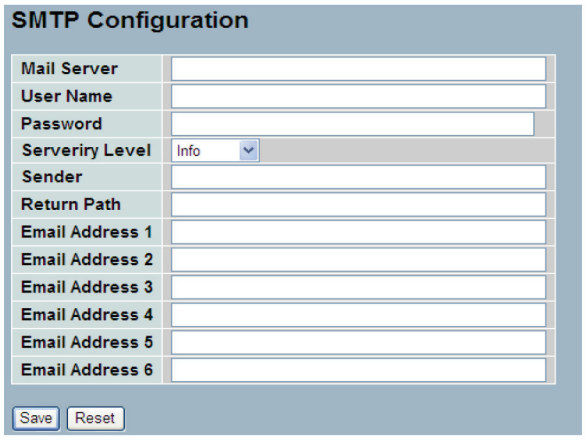


Figure 3-97. The SMTP Configuration screen

Parameter Description

These parameters are displayed on the SMTP Configuration page:

- Mail Server: Specify the IP Address of the server transferring your e-mail.
- Username: Specify the username on the mail server.
- Password: Specify the password on the mail server.
- Sender: To set the mail sender name.
- Return-Path: To set the mail return-path as sender mail address.
- Email Address 1–6: Email address where you would like to receive the alarm message.
- Buttons:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

3.25 UPnP

Universal Plug and Play (UPnP) enables devices to connect seamlessly and to simplify the implementation of networks in home (data sharing, communications, and entertainment) and corporate environments.

Web Interface

To configure UPnP Configuration in the Web interface:

1. Click Configuration, UPnP.
2. Scroll to select the mode to enable or disable.
3. Specify the parameters in each blank field.
4. Click "Save" to save the setting.
5. Click "Reset" to undo any changes made locally and revert to previously saved values.

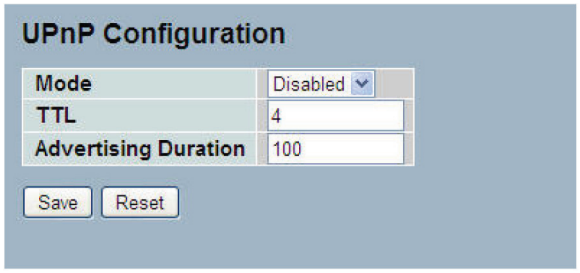


Figure 3-98. The UPnP Configuration screen.

Parameter Description

These parameters are displayed on the UPnP Configuration page:

- Mode: Indicates the UPnP operation mode. Possible modes are:
  - Enabled: Enable UPnP mode operation.
  - Disabled: Disable UPnP mode operation.

  When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed when the mode is disabled.
- TTL: The TTL value is used by UPnP to send SSDP advertisement messages. Valid values range from 1 to 255.
- Advertising Duration: The duration, carried in SSDP packets, is used to inform a control point (or control points) how often it (or they) should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Because of the unreliable nature of UDP, the standard recommends that such refreshing of advertisements should be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval of one-half of the advertising duration minus 30 seconds. Valid values range from 100 to 86400.
- Buttons:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

4. Security

This chapter describes all the switch security configuration tasks to enhance the security of the local network including IP Source Guard, ARP Inspection, DHCP Snooping, AAA, and others.

4.1. IP Source Guard

This section describes how to configure the IP Source Guard detail parameters of the switch. Use the IP Source Guard Configuration screen to configure to enable or disable with the port of the switch.

4.1.1 Configuration

This section describes how to configure the IP Source Guard setting including:

- Mode (Enabled and Disabled)
- Maximum Dynamic Clients (0, 1, 2, Unlimited)

Web Interface

To configure an IP Source Guard in the Web interface:

1. Select "Enabled" in the Mode of IP Source Guard Configuration.
2. Select "Enabled" of the specific port in the Mode column.
3. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Mode of Port Mode Configuration.
4. Click Save.

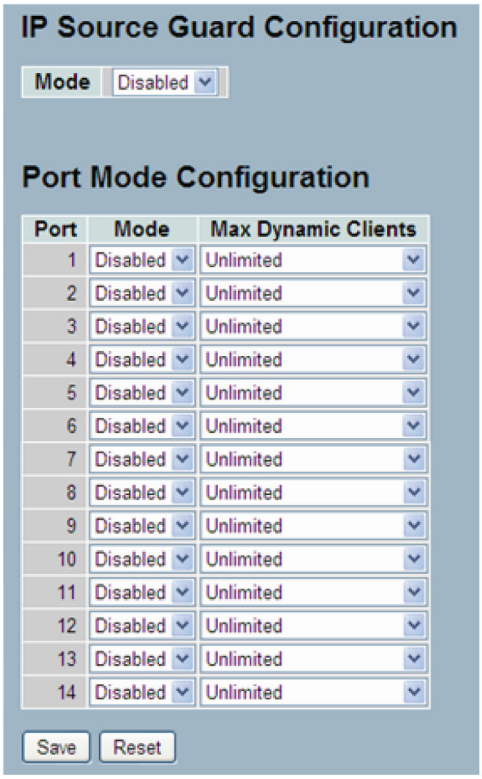


Figure 4-1. The IP Source Guard Configuration screen.

Parameter Description

- **Mode of IP Source Guard Configuration**: Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
- **Port Mode Configuration**: Specify on which ports IP Source Guard is enabled. Only when both Global Mode and Port Mode on a given port are enabled is IP Source Guard enabled on that port.
- **Max Dynamic Clients**: Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means it only allows the IP packets forwarding that are matched in static entries on the specific port.
- Buttons:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

4.1.2 Static Table

This section describes how to configure the Static IP Source Guard Table parameters of the switch. The Static IP Source Guard Table enables you to configure and to manage the entries.

Web Interface

To configure a Static IP Source Guard Table Configuration in the Web interface:

1. Click "Add new entry."
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click "Save."

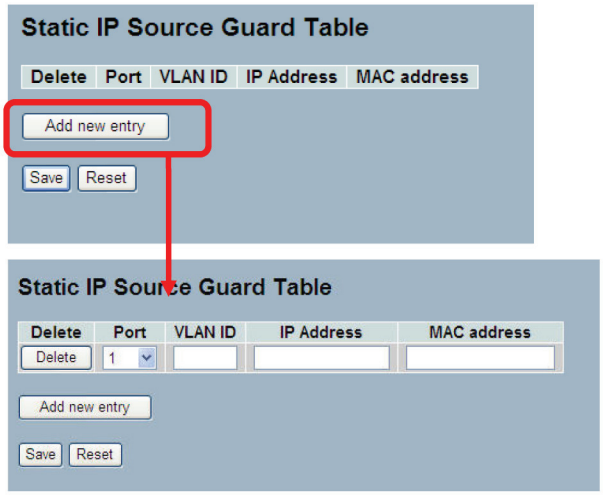


Figure 4-2. The Static IP Source Guard Table screen.

Parameter Description

- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **Port**: The logical port for the settings.
- **VLAN ID**: The VLAN ID for the settings.
- **IP Address**: Valid source IP address.

- **IP Mask**: Used for calculating the allowed network with IP address.
- **MAC address**: Valid source MAC address.
- **Adding new entry**: Click to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click "Save."
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

4.1.3 Dynamic Table

The section describes how to configure the Dynamic IP Source Guard Table parameters of the switch. Use the Dynamic IP Source Guard Table configure to manage the entries.

Web Interface

To configure a Dynamic IP Source Guard Table Configuration in the Web interface:

1. Specify the Start from port, VLAN ID, IP Address, and entries per page.
2. Checked "Auto-refresh".

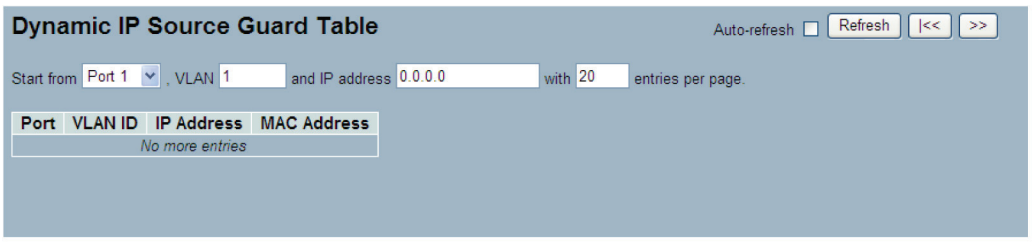


Figure 4-3. The Dynamic IP Source Guard Table screen.

Parameter Description

- **Port**: Switch Port Number for which the entries are displayed.
- **VLAN ID**: VLAN ID in which the IP traffic is permitted.
- **IP Address**: User IP address of the entry.
- **MAC Address**: Source MAC address.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icons, upper right (Refresh, <<, >>)**: Click to refresh the Dynamic IP Source Guard Table manually. Click << or >> to scroll to the next entry on the table.

4.2 ARP Inspection

The section describes to configure the ARP Inspection parameters of the switch. Use the ARP Inspection configure to manage the ARP table.

4.2.1 Configuration

This section describes how to configure ARP Inspection setting including:

- Mode (Enabled and Disabled).
- Port (Enabled and Disabled).

Web Interface

To configure an ARP Inspection Configuration in the Web interface

1. Select "Enabled" in the Mode of ARP Inspection Configuration.
2. Select "Enabled" for the specific ports to enable in the Mode of Port Mode Configuration.
3. Click "Save."

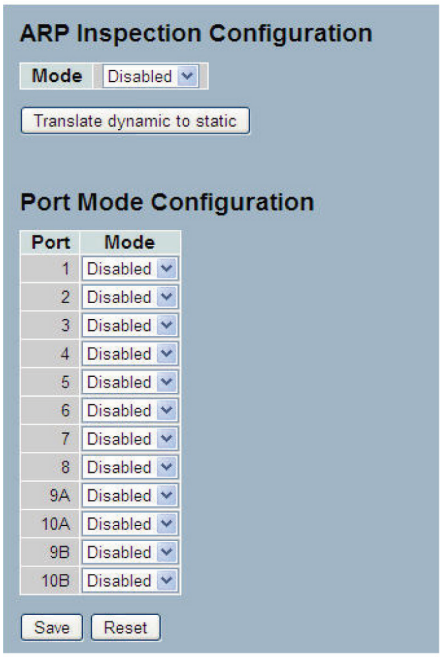


Figure 4-4. The ARP Inspection Configuration screen.

Parameter Description

- Mode of ARP Inspection Configuration: Enable or disable the Global ARP Inspection.
- Port Mode Configuration: Specify ARP Inspection is enabled on which ports. ARP Inspection is enabled on this given port only when both Global Mode and Port Mode on a given port are enabled.
- Buttons:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.2 Static Table

This section describes how to configure the Static ARP Inspection Table parameters of the switch.

Web Interface

To configure a Static ARP Inspection Table Configuration in the Web interface:

1. Click "Add new entry".
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click "Save."

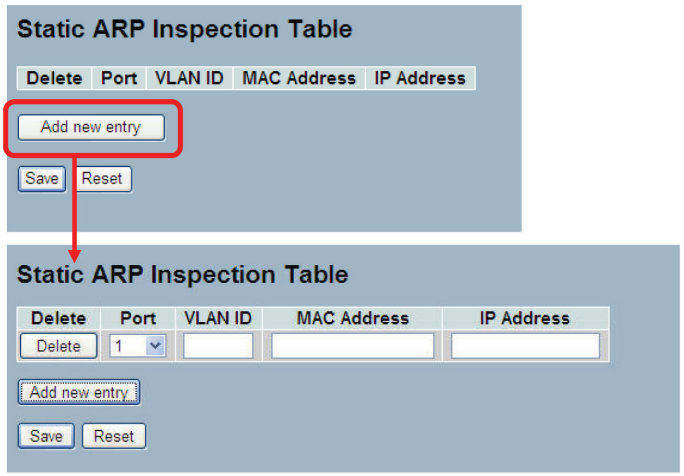


Figure 4-5. The Static ARP Inspection Table

Parameter Description

- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **Port**: The logical port for the settings.
- **VLAN ID**: The VLAN ID for the settings.
- **MAC Address**: Allowed Source MAC address in ARP request packets.
- **IP Address**: Allowed Source IP address in ARP request packets.
- **Adding new entry**: Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click "Save."
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.3 Dynamic Table

This section describes how to configure the Dynamic ARP Inspection Table parameters. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Web Interface

To configure a Dynamic ARP Inspection Table Configuration in the Web interface:

1. Specify the Start from port, VLAN ID, MAC Address, IP Address, and entries per page.
2. Check "Auto-refresh".

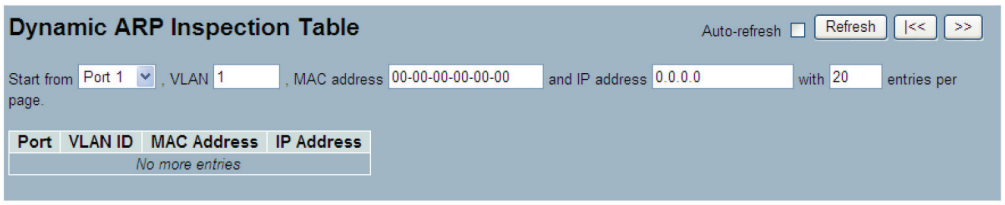


Figure 4-6. The Dynamic ARP Inspection Table screen.

Parameter Description

- **Port**: Switch Port Number for which the entries are displayed.
- **VLAN ID**: VLAN-ID in which the ARP traffic is permitted.
- **MAC Address**: User MAC address of the entry.
- **IP Address**: User IP address of the entry.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icons, upper right (Refresh, |<<, >>)**: Click Refresh to refresh the Dynamic ARP Inspection Table manually. Press |<< or >> to scroll to the next entry on the table.

4.3 DHCP Snooping

The section describes how to configure the DHCP Snooping parameters of the switch, for the purpose of preventing attackers from adding their own DHCP servers to the network.

4.3.1 Configuration

This section describes how to configure the DHCP Snooping setting including:

- Snooping Mode (Enabled and Disabled)
- Port Mode Configuration (Trusted, Untrusted)

Web Interface

To configure DHCP Snooping in the Web interface:

1. Select "Enabled" in the Mode of DHCP Snooping Configuration.
2. Select "Trusted" of the specific port in the Mode of Port Mode Configuration.
3. Click "Save."

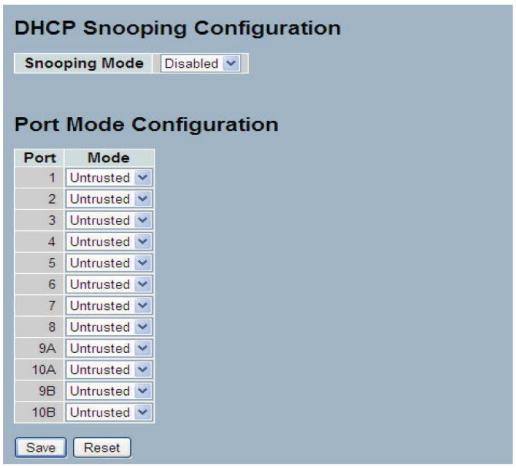


Figure 4-7. The DHCP Snooping Configuration screen.

Parameter Description

- Snooping Mode: Indicates the DHCP snooping mode operation. Possible modes are:
  - Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.
  - Disabled: Disable DHCP snooping mode operation.
- Port Mode: Indicates the DHCP snooping port mode. Possible port modes are:
  - Trusted: Configures the port as trusted source of the DHCP messages.
  - Untrusted: Configures the port as untrusted source of the DHCP messages.
- Buttons:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.2 Statistics

This section describes how to display the DHCP snooping port statistics. The statistics show only packet counters when DHCP snooping mode is enabled and relay mode is disabled. They don't count the DHCP packets for a DHCP client.

Web Interface

To configure DHCP Snooping Statistics in the Web interface:

1. Specify the Port which you want to monitor.
2. Check "Auto-refresh".

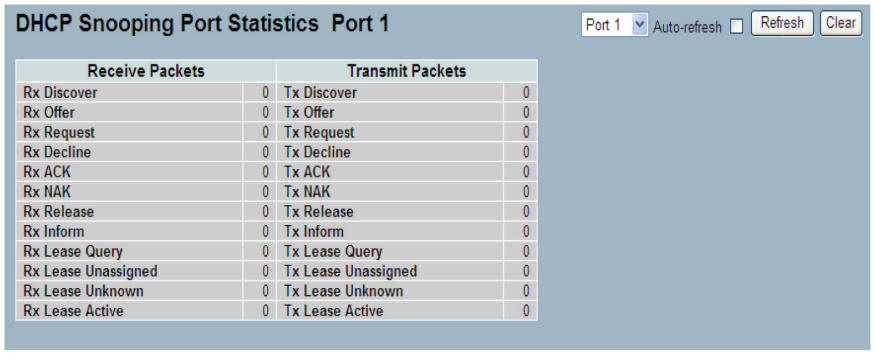


Figure 4-8. DHCP Snooping Port Statistics screen.

Parameter Description

- **Rx and Tx Discover**: The number of discover (option 53 with value 1) packets received and transmitted.
- **Rx and Tx Offer**: The number of offer (option 53 with value 2) packets received and transmitted.
- **Rx and Tx Request**: The number of request (option 53 with value 3) packets received and transmitted.
- **Rx and Tx Decline**: The number of decline (option 53 with value 4) packets received and transmitted.
- **Rx and Tx ACK**: The number of ACK (option 53 with value 5) packets received and transmitted.
- **Rx and Tx NAK**: The number of NAK (option 53 with value 6) packets received and transmitted.
- **Rx and Tx Release**: The number of release (option 53 with value 7) packets received and transmitted.
- **Rx and Tx Inform**: The number of inform (option 53 with value 8) packets received and transmitted.
- **Rx and Tx Lease Query**: The number of lease query (option 53 with value 10) packets received and transmitted.
- **Rx and Tx Lease Unassigned**: The number of lease unassigned (option 53 with value 11) packets received and transmitted.
- **Rx and Tx Lease Unknown**: The number of lease unknown (option 53 with value 12) packets received and transmitted.
- **Rx and Tx Lease Active**: The number of lease active (option 53 with value 13) packets received and transmitted.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icons, upper right (Refresh, Clear)**: Click to refresh DHCP Snooping Port Statistics manually. Press "clear" to clear all new entries.

4.4 DHCP Relay

The section describes how to forward DHCP requests to another specific DHCP servers via DHCP relay. The DHCP servers may be on another network.

4.4.1 Configuration

This section describes how to configure DHCP Relay setting including:

- Relay Mode (Enabled and Disabled)
- Relay Server IP setting
- Relay Information Mode (Enabled and Disabled)
- Relay Information Mode Policy (Replace, Keep and Drop)

Web Interface

To configure a DHCP Relay in the Web interface:

1. Select "Enabled" in the Relay Mode of DHCP Relay Configuration.
2. Specify Relay Server IP address.
3. Select "Enabled" in the Relay Information Mode of DHCP Relay Configuration.
4. Specify Relay (Replace, Keep and Drop) in the Relay Information Mode of DHCP Relay Configuration.
5. Click Save.

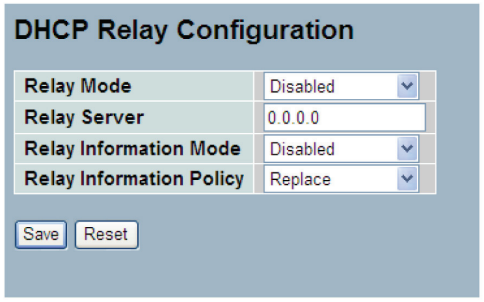


Figure 4-9. The DHCP Relay Configuration screen.

Parameter Description

- **Relay Mode**: Indicates the DHCP relay mode operation. Possible modes are:
  - Enabled:Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.
  - Disabled: Disable DHCP relay mode operation.
- **Relay Server**: Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain.
- **Relay Information Mode**: Indicates the DHCP relay information mode option operation. Possible modes are:
  - Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

    Disabled: Disable DHCP relay information mode operation.

- **Relay Information Policy**: Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if agent receives a DHCP message that already contains relay agent information, it will enforce the policy. And it only works under DHCP if relay information operation mode is enabled. Possible policies are:
  - Replace:Replace the original relay information when a DHCP message that already contains it is received.
  - Keep: Keep the original relay information when a DHCP message that already contains it is received.
  - Drop: Drop the package when a DHCP message that already contains relay information is received.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

4.4.2 Statistics

This section describes how to show the DHCP Relay Statistics information of the switch. The statistics show both Server and Client packet counters when DHCP Relay mode is enabled.

Web Interface

To configure a DHCP Snooping Statistics Configuration in the Web interface:

1. Check "Auto-refresh."

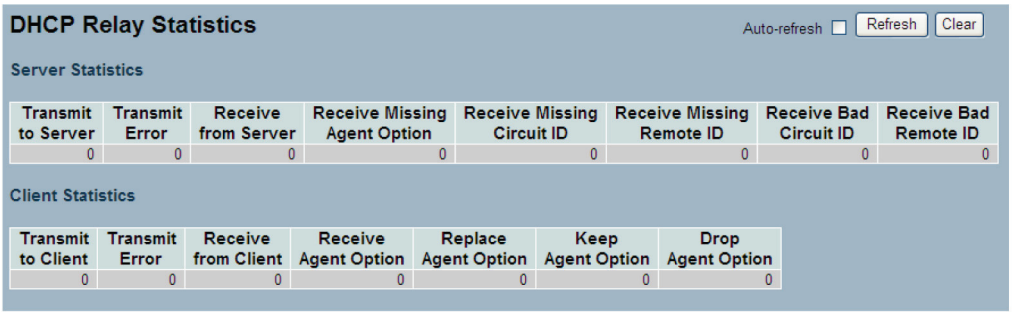


Figure 4-10. The DHCP Relay Statistics screen.

Parameter Description

- **Transmit to Server**: The number of packets that are relayed from client to server.
- **Transmit Error**: The number of packets that resulted in errors while being sent to clients.
- **Receive from Server**: The number of packets received from server.
- **Receive Missing Agent Option**: The number of packets received without agent information options.
- **Receive Missing Circuit ID**: The number of packets received with the Circuit ID option missing.
- **Receive Missing Remote ID**: The number of packets received with the Remote ID option missing.
- **Receive Bad Circuit ID**: The number of packets whose Circuit ID option did not match known circuit ID.
- **Receive Bad Remote ID**: The number of packets whose Remote ID option did not match known remote ID.

Client Statistics

- **Transmit to Client**: The number of relayed packets from server to client.
- **Transmit Error**: The number of packets that resulted in error while being sent to servers.
- **Receive from Client**: The number of received packets from server.
- **Receive Agent Option**: The number of received packets with relay agent information option.
- **Replace Agent Option**: The number of packets which were replaced with relay agent information option.
- **Keep Agent Option**: The number of packets whose relay agent information was retained.
- **Drop Agent Option**: The number of packets that were dropped which were received with relay agent information.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icons, upper right (Refresh, Clear)**: Click to refresh the DHCP Relay Statistics manually. Press clear to clear all new entries.

4.5 NAS

This section describes how to configure the NAS parameters of the switch. The NAS server can be used to connect users to a variety of resources including Internet access, conference calls, printing documents on shared printers, or by simply logging on to the Internet.

4.5.1 Configuration

This section describes how to configure the NAS setting of the IEEE 802.1X, MAC-based authentication system and port settings. The NAS configuration consists of two sections: system-wide and port-wide.

Web Interface

To configure a System Configuration of Network Access Server in the Web interface:

1. Select "Enabled" in the Mode of Network Access Server Configuration.
2. Check Reauthentication Enabled.
3. Set Reauthentication Period (default is 3600 seconds).
4. Set EAPOL Timeout (default is 30 seconds).
5. Set Aging Peroid (default is 300 seconds).
6. Set Hold Time (default is 10 seconds).
7. Check "RADIUS-Assigned QoS Enabled."
8. Check "RADIUS-Assigned VLAN Enabled."
9. Check "Guest VLAN Enabled."
10. Specify Guest VLAN ID.
11. Specify Max. Reauth. Count.
12. Check "Allow Guest VLAN if EAPOL Seen."
13. Click "Save."

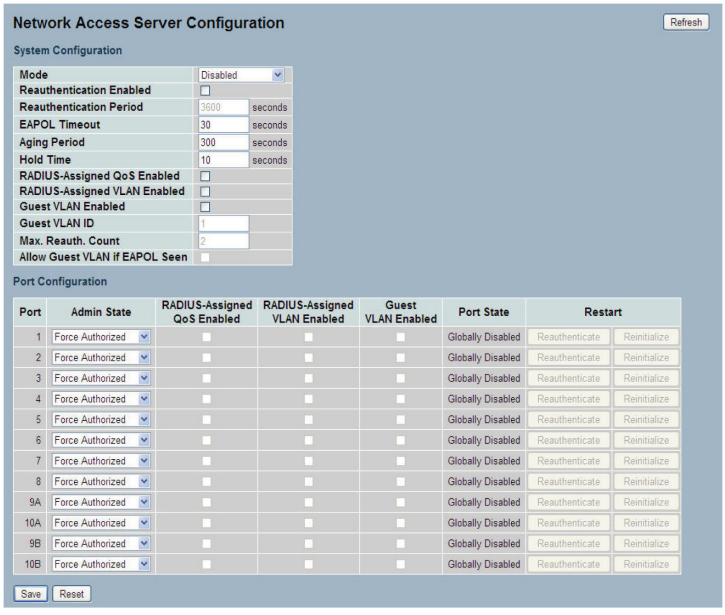


Figure 4-11. The Network Access Server Configuration screen.

Parameter Description

- **Mode**: Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
- **Reauthentication Enabled**: If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

  For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).
- **Reauthentication Period**: Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range of 1 to 3600 seconds.
- **EAPOL Timeout**: Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.
- **Aging Period**: This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

  - Single 802.1X

  - Multi 802.1X

  - MAC-Based Auth.

  When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1,000,000 seconds.

  If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

  For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
- **Hold Time**: This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: Single 802.1X, Multi 802.1X, and MAC-Based Auth.

  If a client is denied access—either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration --> Security --> AAA" page)—the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

  The Hold Time can be set to a number between 10 and 1,000,000 seconds.
- **RADIUS-Assigned QoS Enabled**: RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

  The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto settings determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

- **RADIUS-Assigned VLAN Enabled**: RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).

  The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

- **Guest VLAN Enabled**: A Guest VLAN is a special VLAN—typically with limited network access—on which 802.1Xunaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

  The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

- **Guest VLAN ID**: This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].

- **Max. Reauth. Count**: The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].

- **Allow Guest VLAN if EAPOL Seen**: The switch remembers if an EAPOL frame has been received on the port for the lifetime of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the lifetime of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the lifetime of the port.

  The value can only be changed if the Guest VLAN option is globally enabled.

- **Port Configuration**: The table has one row for each port on the selected switch and a number of columns, which are:

  - Port: The port number for which the configuration below applies.

  - Admin State: If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

  - Force Authorized: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

  - Force Unauthorized: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

- **Port-based 802.1X**: In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

  When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

NOTE: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead).

Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel ongoing backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant.

And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

- **Single 802.1X**: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggyback on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.
- **Multi 802.1X**: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggyback on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.

  Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

  In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination to wake up any supplicants that might be on the port.

  The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.
- **MAC-based Auth.**: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xxxx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

  When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a third party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users—equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **RADIUS-Assigned QoS Enabled**: When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS assigned).

  This option is only available for single-client modes, i.e.

  - Port-based 802.1X

  - Single 802.1X

  RADIUS attributes used in identifying a QoS Class:

  Refer to the written documentation for a description of the RADIUS attributes needed to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

  Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

  - All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].

- **RADIUS-Assigned VLAN Enabled**: When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

  If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

  This option is only available for single-client modes, i.e.

  - Port-based 802.1X

  - Single 802.1X

  For troubleshooting VLAN assignments, use the "Monitor --> VLANs --> VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

  RADIUS attributes used in identifying a VLAN ID: RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

  - The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.

  - The switch looks for the first set of these attributes that have the same Tag value and fulfill the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):

    - Value of Tunnel-Medium-Type must be set to “IEEE-802” (ordinal 6).

- Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
- Value of Tunnel-Private-Group-ID must be a string of ASCII characters in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

- **Guest VLAN Enabled**: When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

  This option is only available for EAPOL-based modes, i.e.:

  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X

  For troubleshooting VLAN assignments, use the "Monitor --> VLANs --> VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

  Guest VLAN Operation:

  When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meantime, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

  Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

  While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

- **Port State**: The current state of the port. It can undertake one of the following values:

  Globally Disabled: NAS is globally disabled.

  Link Down: NAS is globally enabled, but there is no link on the port.

  Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

  Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

  X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

- **Restart**: Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

  Clicking these buttons will not cause settings changed on the page to take effect.

  Reauthenticate: Schedules a reauthentication whenever the quiet period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.

  The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Reinitialize: Forces a reinitialization of the clients on the port—and thereby a reauthentication—immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

- Buttons:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.
- Icon, upper right of screen (Refresh): Click to refresh the NAS Configuration information manually.

4.5.2 Switch Status

This section describes how to display port NAS status information for the switch. The status includes Admin State, Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

Web Interface

To configure a NAS Switch Status Configuration in the Web interface: Check "Auto-refresh".

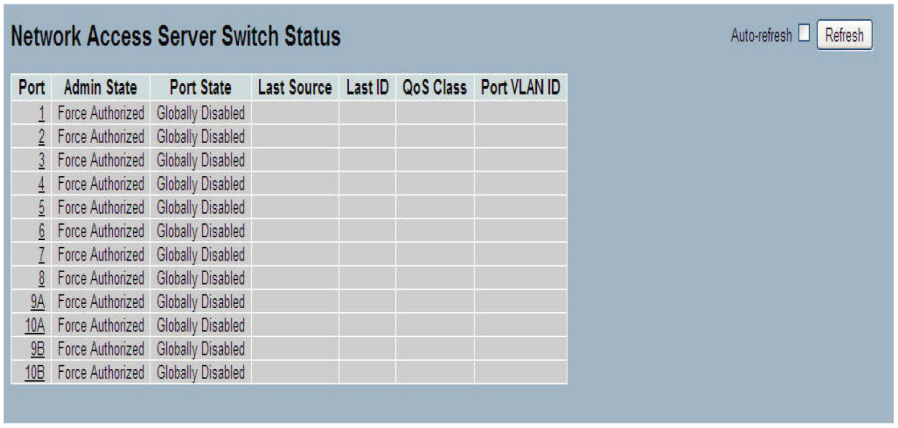


Figure 4-12. The Network Access Server Switch Status screen.

Parameter Description

- **Port**: The switch port number. Click to navigate to detailed NAS statistics for this port.
- **Admin State**: The port's current administrative state. Refer to NAS Admin State for a description of possible values.
- **Port State**: The current state of the port. Refer to NAS Port State for a description of the individual states.
- **Last Source**: The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
- **Last ID**: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
- **QoS Class**: QoS Class assigned to the port by the RADIUS server if enabled.
- **Port VLAN ID**: The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the NAS Switch Status information manually.

4.5.3 Port Status

This section provides detailed informationon how to display NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication.

Web Interface

To configure a NAS Port Status Configuration in the Web interface:

1. Specify the Port you want to check.
2. Check "Auto-refresh".

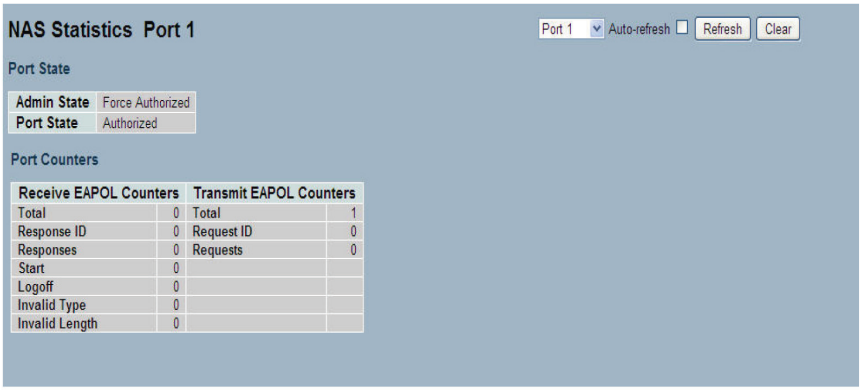


Figure 4-13. The NAS Statistics screen.

Parameter Description

Port State

- **Admin State**: The port's current administrative state. Refer to NAS Admin State for a description of possible values.
- **Port State**: The current state of the port. Refer to NAS Port State for a description of the individual states.
- **QoS Class**: The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
- **Port VLAN ID**: The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

  If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

  If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Port Counters

- **EAPOL Counters**: These supplicant frame counters are available for the following administrative states:
  - Force Authorized
  - Force Unauthorized
  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X
- **Backend Server Counters**: These backend (RADIUS) frame counters are available for the following administrative states:
  - Port-based 802.1X
  - Single 802.1X

- Multi 802.1X
- MAC-based Auth.

- **Last Supplicant/Client Info**: Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:
  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X
  - MAC-based Auth.

Selected Counters

- **Selected Counters**: The Selected Counters table is visible when the port is in one of the following administrative states:
- **Multi 802.1X**
- **MAC-based Auth.**: The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC addresses from the table described below.

Attached MAC Addresses

- **Identity**: Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.

  This column is not available for MAC-based Auth.

- **MAC Address**: For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client.

  Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.

VLAN ID

This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

- **State**: The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.
- **Last Authentication**: Shows the date and time of the last authentication of the client (successful as well as unsuccessful).
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icons, upper right of screen (Refresh, Clear)**: Click to refresh the NAS Statistics information manually. Click Clear to revert top reviously-saved values.

4.6 AAA

This section shows you how to use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

4.6.1 Configuration

This section describes how to configure an AAA setting of TACACS+ or RADIUS server.

Web Interface

To configure a Common Configuration of AAA in the Web interface:

1. Set Timeout (Default is 15 seconds).
2. Set Dead Time (Default is 300 seconds).

To configure a TACACS+ Authorization and Accounting Configuration of AAA in the Web interface:

1. Select "Enabled" in the Authorization.
2. Select "Enabled" in the Failback to Local Authorization.
3. Select "Enabled" in the Account.

To configure a RADIUS Authentication Server Configuration of AAA in the Web interface:

1. Check "Enabled".
2. Specify IP address or Hostname for Radius Server.
3. Specify Authentication Port for Radius Server (Default is 1812).
4. Specify the Secret with Radius Server.

To configure a RADIUS Accounting Server Configuration of AAA in the Web interface:

1. Check "Enabled".
2. Specify IP address or Hostname for Radius Server.
3. Specify Accounting Port for Radius Server (Default is 1813).
4. Specify the Secret with Radius Server.

To configure a TACACS+ Authentication Server Configuration of AAA in the Web interface:

1. Check "Enabled".
2. Specify IP address or Hostname for TACACS+ Server.
3. Specify Authentication Port for TACACS+ Server (Default is 49).
4. Specify the Secret with TACACS+ Server.

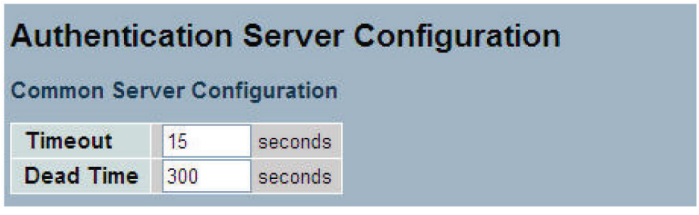


Figure 4-14. The Common Server Configuration screen.

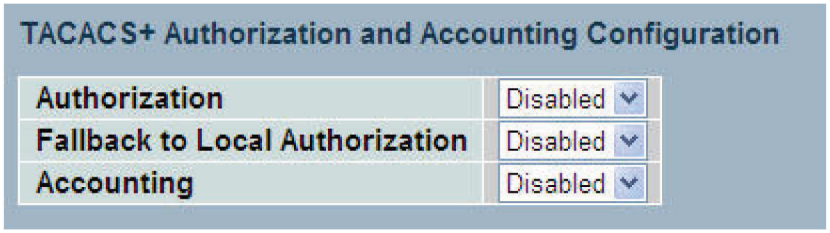


Figure 4-15. The TACACS+ Authorization and Accounting Configuration screen.

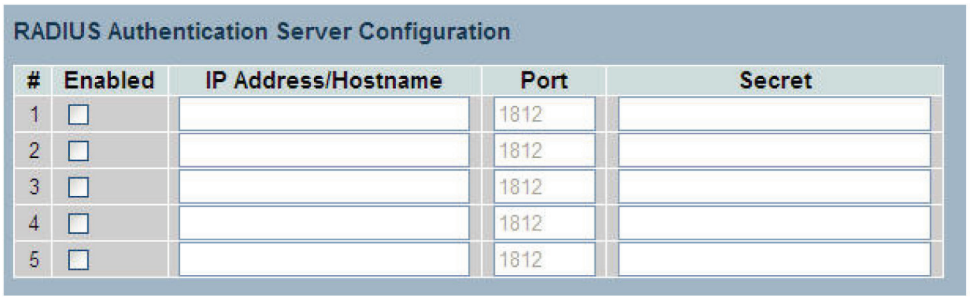


Figure 4-16. The RADIUS Authentication Configuration screen.

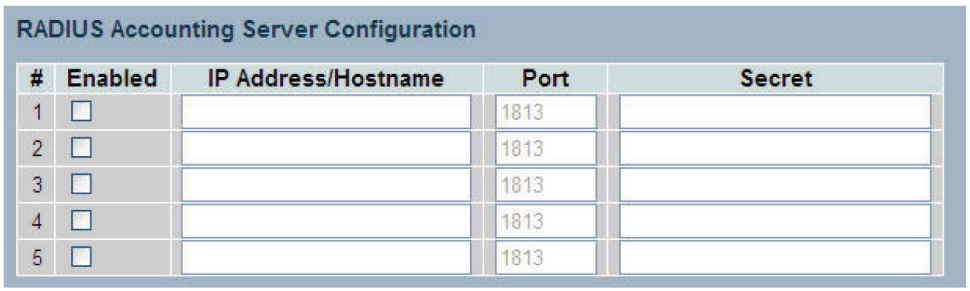


Figure 4-17. The RADIUS Accounting Configuration screen.

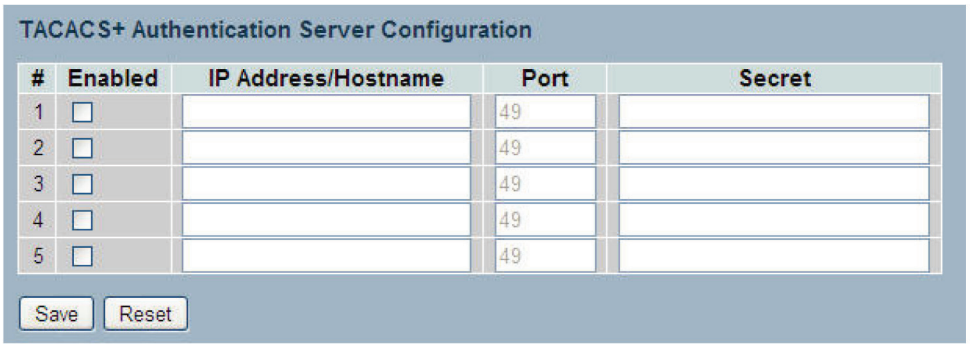


Figure 4-18. The TACACS+ Authentication Configuration screen.

Parameter Description

- **Timeout**: The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any).

  RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

- **Dead Time**: The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

  Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

RADIUS Authentication Server Configuration

The table has one row for each RADIUS Authentication Server and a number of columns, which are:

- **#**: The RADIUS Authentication Server number for which the configuration below applies.
- **Enabled**: Enable the RADIUS Authentication Server by checking this box.
- **IP Address/Hostname**: The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.
- **Port**: The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
- **Secret**: The secret—up to 29 characters long—shared between the RADIUS Authentication Server and the switch.

RADIUS Accounting Server Configuration

The table has one row for each RADIUS Accounting Server and a number of columns, which are:

- **#**: The RADIUS Accounting Server number for which the configuration below applies.
- **Enabled**: Enable the RADIUS Accounting Server by checking this box.
- **IP Address/Hostname**: The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.
- **Port**: The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
- **Secret**: The secret—up to 29 characters long—shared between the RADIUS Accounting Server and the switch.

TACACS+ Authentication Server Configuration

The table has one row for each TACACS+ Authentication Server and a number of columns, which are:

- **#**: The TACACS+ Authentication Server number for which the configuration below applies.
- **Enabled**: Enable the TACACS+ Authentication Server by checking this box.
- **IP Address/Hostname**: The IP address or hostname of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.

- **Port**: The TCP port to use on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.
- **Secret**: The secret—up to 29 characters long—shared between the TACACS+ Authentication Server and the switch.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

4.6.2 RADIUS Overview

This section provides an overview of the RADIUS Authentication and Accounting servers status.

Web Interface

To configure a RADIUS Overview Configuration in the Web interface: Check "Auto-refresh."

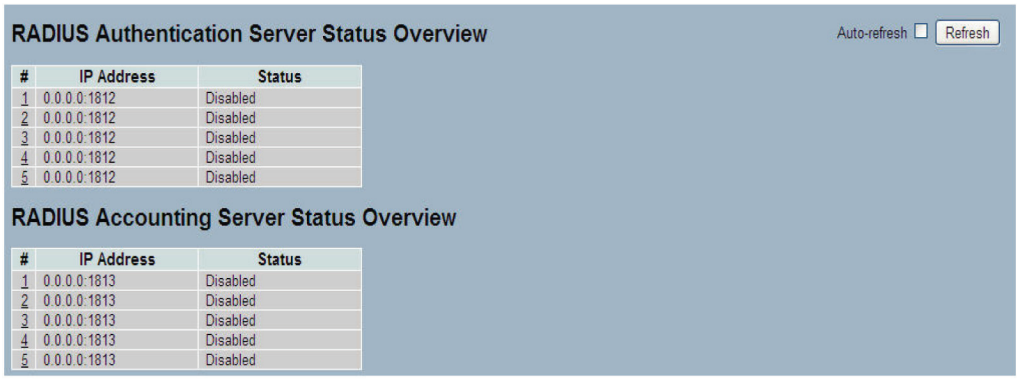


Figure 4-19. The RADIUS Authentication Server Status Overview screen

Parameter Description

RADIUS Authentication Servers

- **#**: The RADIUS server number. Click to navigate to detailed statistics for this server.
- **IP Address**: The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
- **State**: The current state of the server. This field takes one of the following values:
  - Disabled: The server is disabled.
  - Not Ready: The server is enabled, but IP communication is not yet up and running.
  - Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
  - Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Servers

- **#**: The RADIUS server number. Click to navigate to detailed statistics for this server.
- **IP Address**: The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
- **State**: The current state of the server. This field takes one of the following values:

- Disabled: The server is disabled.
- Not Ready: The server is enabled, but IP communication is not yet up and running.
- Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
- Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get reenabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

• **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.

• **Icon, upper right of screen (Refresh)**: Click to refresh the RADIUS Status information manually.

4.6.3 RADIUS Details

This section shows you a detailed statistics of the RADIUS Authentication and Accounting servers. The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Web Interface

To configure a RADIUS Details Configuration in the Web interface:

1. Specify which port you want to check.
2. Check "Auto-refresh."

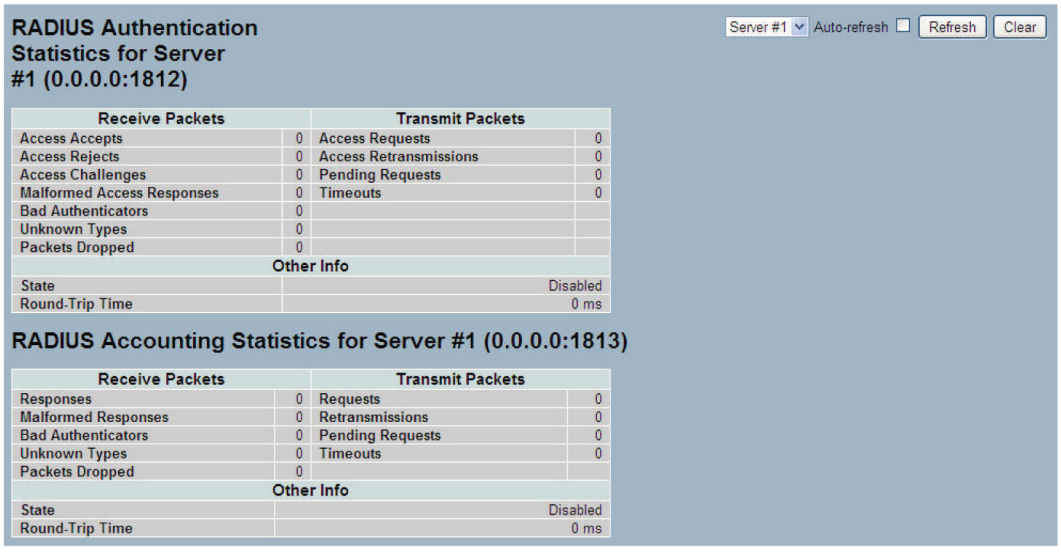


Figure 4-20. The RADIUS Authentication Statistics for Server screen.

Parameter Description

• **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.

• **Icons, upper right of screen (Refresh, Clear)**: Click to refresh the RADIUS Statistics information manually; click Clear to clear all new entries.

4.7 Port Security

This section demonstrates how to configure the Port Security settings of the Switch. Use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

4.7.1 Limit Control

This section demonstrates how to configure the Port Security settings of the Switch. Use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

Web Interface

To configure a System Configuration of Limit Control in the Web interface:

1. Select "Enabled" in the Mode of System Configuration.
2. Check Aging Enabled.
3. Set Aging Period (Default is 3600 seconds).

To configure a Port Configuration of Limit Control in the Web interface:

1. Select "Enabled" in the Mode of Port Configuration.
2. Specify the maximum number of MAC addresses in the Limit of Port Configuration.
3. Set Action (Trap, Shutdown, Trap & Shutdown).
4. Click "Save."

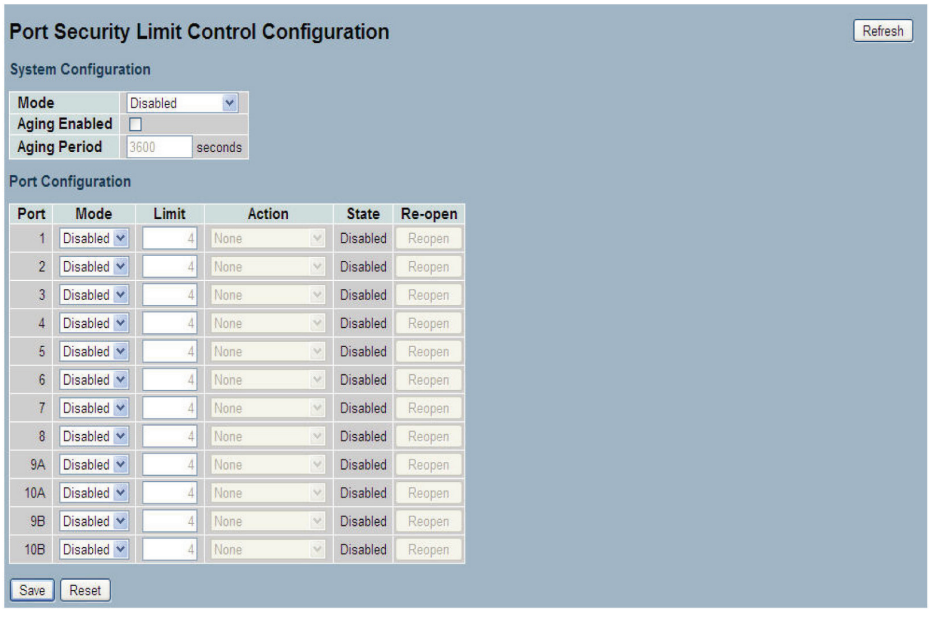


Figure 4-21. The Port Security Limit Control Configuration

Parameter Description

System Configuration

- **Mode**: Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

- **Aging Enabled**: If checked, secured MAC addresses are subject to aging as discussed under Aging Period.
- **Aging Period**: If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

  The Aging Period can be set to a number between 10 and 10,000,000 seconds.

  To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a third party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

The table has one row for each port on the selected switch and a number of columns, which are:

- **Port**: The port number to which the configuration below applies.
- **Mode**: Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.
- **Limit**: The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
- **Action**: If Limit is reached, the switch can take one of the following actions:
  - None: Do not allow more than Limit MAC addresses on the port, but take no further action.
  - Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent everytime the limit gets exceeded.
  - Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

    1) Boot the switch,

    2) Disable and re-enable Limit Control on the port or the switch,

    3) Click the Reopen button.
  - Trap and Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.
- **State**: This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:
  - Disabled: Limit Control is either globally disabled or disabled on the port.
  - Ready: The limit is not yet reached. This can be shown for all actions.
  - Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.

- Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

- **Re-open Button**: If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section.

NOTE: That clicking the reopen button causes the page to be refreshed, so unsaved changes will be lost.

- **Icon, upper right of screen (Refresh)**: Click to refresh the Port Security information manually.

- **Buttons**:

  - Save: Click to save changes.

  - Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.2 Switch Status

This section shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules—the user modules. When a user module has enabled port security on a port, the port is setup for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections—one with a legend of user modules and one with the actual port status.

Web Interface

To configure a Port Security Switch Status Configuration in the Web interface: Check "Auto-refresh."

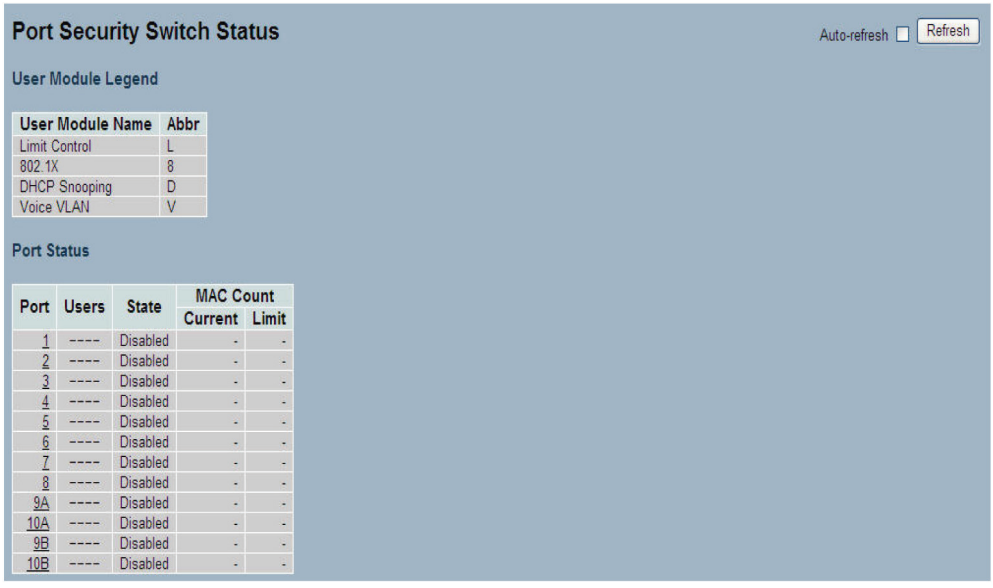


Figure 4-22. The Port Security Switch Status screen.

Parameter Description

- **User Module Legend**: The legend shows all user modules that may request Port Security services.

- **User Module Name**: The full name of a module that may request Port Security services.

- **Abbr**: A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

- Port Status: The table has one row for each port on the selected switch and a number of columns, which are:
- Port: The port number for which the status applies. Click the port number to see the status for this particular port.
- Users: Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
- State: Shows the current state of the port. It can take one of four values:
  - Disabled: No user modules are currently using the Port Security service.
  - Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.
  - Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.
  - Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web page.
- MAC Count (Current, Limit): The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

  If no user modules are enabled on the port, the Current column will show a dash (-).

  If the Limit Control user module is not enabled on the port, the Limit column will show a dash (—).

  Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (—) will be shown.
- Auto-refresh: Check the auto-refresh box to set the unit to refresh information automatically.
- Icon, upper right of screen (Refresh): Click to refresh the Port Security Switch Status information manually.

4.7.3 Port Status

This section shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules, including the user modules. When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Web Interface

To configure a Port Security Switch Status Configuration in the Web interface:

1. Specify the Port which you want to monitor.
2. Check "Auto-refresh."

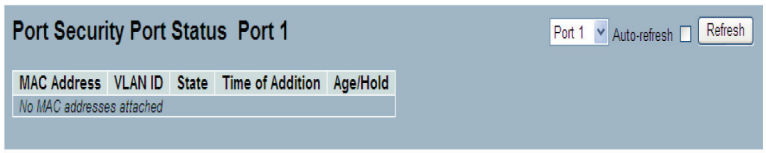


Figure 4-23. The Port Security Port Status screen.

Parameter Description

- **MAC Address & VLAN ID**: The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.
- **State**: Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
- **Time of Addition**: Shows the date and time when this MAC address was first seen on the port.
- **Age/Hold**: If at least one user module has decided to block this MAC address, it will stay in the locked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (—) will be shown.
- **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.
- **Icon, upper right of screen (Refresh)**: Click to refresh the Port Security Port Status information manually.

4.8 Access Management

This section shows how to configure access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN, or over the Internet.

4.8.1 Configuration

This section shows how to configure access management table of the switch. The maximum entry number is 16. If the application's type matches any one of the access management entries, it will allow access to the switch.

Web Interface

To configure a Access Management Configuration in the Web interface:

1. Select "Enabled" in the Mode of Access Management Configuration.
2. Click "Add new entry."
3. Specify the Start IP Address, End IP Address.
4. Check Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
5. Click "Save."

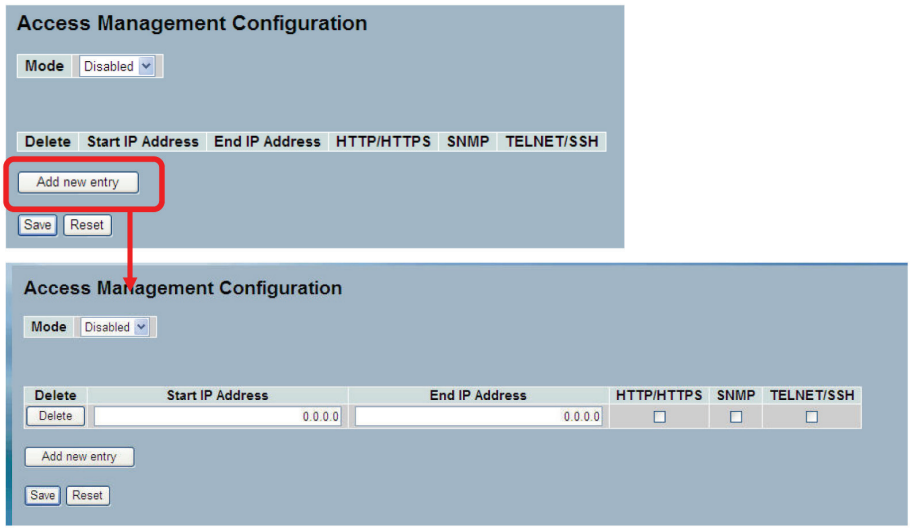


Figure 4-24. The Access Management Configuration screen.

Parameter Description

- **Mode**: Indicates the access management mode operation. Possible modes are:
  - Enabled: Enable access management mode operation.
  - Disabled: Disable access management mode operation.
- **Delete**: Check to delete the entry. It will be deleted during the next save.
- **Start IP address**: Indicates the start IP address for the access management entry.
- **End IP address**: Indicates the end IP address for the access management entry.
- **HTTP/HTTPS**: Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
- **SNMP**: Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.
- **TELNET/SSH**: Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

• Buttons:

- Save: Click to save changes.

- Reset: Click to undo any changes made locally and revert to previously saved values.

4.8.2 Statistics

This section shows you a detailed statistics of the Access Management including HTTP, HTTPS, SSH. TELNET, ans SSH.

Web Interface

To configure an Assess Management Statistics in the Web interface: Check "Auto-refresh."

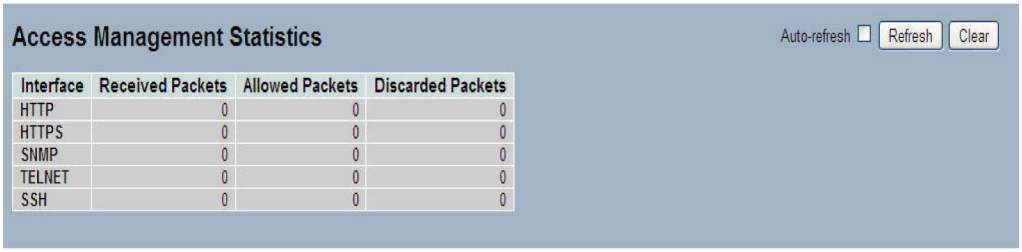


Figure 4-25. The Access Management Statistics screen.

Parameter Description

• **Interface**: The interface type through which the remote host can access the switch.

• **Received Packets**: Number of received packets from the interface when access management mode is enabled.

• **Allowed Packets**: Number of allowed packets from the interface when access management mode is enabled

• **Discarded Packets**: Number of discarded packets from the interface when access management mode is enabled.

• **Auto-refresh**: Check the auto-refresh box to set the unit to refresh information automatically.

• **Icons, upper right (Refresh, Clear)**: Click to refresh the Access Management Statistics information manually. Press clear to clear all new entries and revert to saved values.

4.9 SSH

This section shows how to use SSH (Secure SHell) to securely access the Switch. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

Web Interface

To configure a SSH Configuration in the Web interface:

1. Select "Enabled" in the Mode of SSH Configuration.
2. Click "Save."

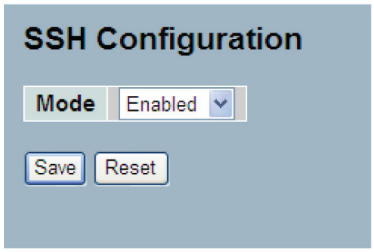


Figure 4-26. The SSH Configuration screen:

Parameter Description

- **Mode**: Indicates the SSH mode operation. Possible modes are:
  - Enabled: Enable SSH mode operation.
  - Disabled: Disable SSH mode operation.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

4.10 HTTPS

This section shows how to use HTTPS to securely access the Switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

Web Interface

To configure a HTTPS Configuration in the Web interface:

1. Select "Enabled" in the Mode of HTTPS Configuration.
2. Select "Enabled" in the Automatic Redirect of HTTPS Configuration.
3. Click "Save."

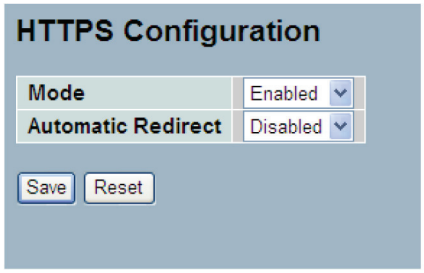


Figure 4-27. The HTTPS Configuration screen

Parameter Description

- **Mode**: Indicates the HTTPS mode operation. Possible modes are:
  - Enabled: Enable HTTPS mode operation.
  - Disabled: Disable HTTPS mode operation.
- **Automatic Redirect**: Indicates the HTTPS redirect mode operation. Automatically redirect Web browser to HTTPS when HTTPS mode is enabled. Possible modes are:
  - Enabled: Enable HTTPS redirect mode operation.
  - Disabled: Disable HTTPS redirect mode operation.

4.11 Authentication Method

This section shows how to configure a user with authentication when logging in to the switch via one of the management client interfaces.

Web Interface

To configure a Authentication Method Configuration in the Web interface:

1. Specify the Client (Console, Telnet, SSH, Web) you want to monitor.
2. Specify the Authentication Method (None, Local, RADIUS, TACACS+)
3. Check "Fallback."
4. Click "Save."

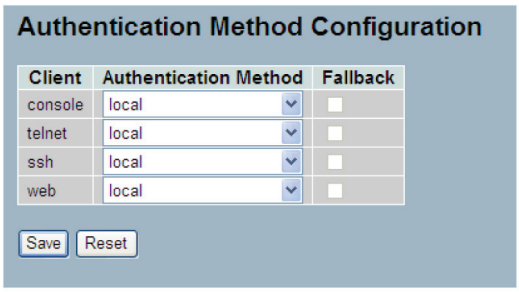


Figure 4-28. Authentication Method Configuration screen.

Parameter Description

- **Client**: The management client for which the configuration below applies.
- **Authentication Method**: Authentication Method can be set to one of the following values:
  - none : authentication is disabled and login is not possible.
  - local : use the local user database on the switch for authentication.
  - radius : use a remote RADIUS server for authentication.
  - tacacs+ : use a remote TACACS+ server for authentication.
- **Fallback**: Enable fallback to local authentication by checking this box. If none of the configured authentication servers is alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to a value other than 'none' or 'local'.
- **Buttons**:
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

5. Maintenance

This chapter describes all the switch Maintenance configuration tasks to enhance the performance of local network including Restart Device, Firmware upgrade, Save/Restore, Import/Export, and Diagnostics.

5.1 Restart Device

This section describes how to restart the switch for any maintenance needs. Any configuration files or scripts saved in the switch should still be available after restart.

Web Interface

To configure a Restart Device Configuration in the Web interface:

1. Ckick "Restart Device."
2. Click "Yes."

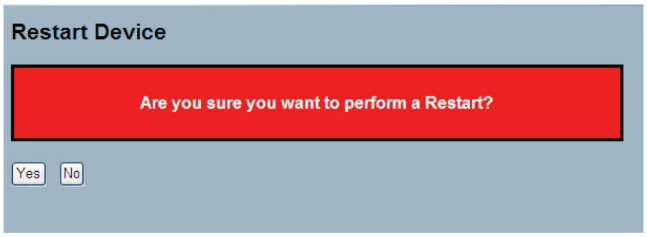


Figure 5-1. The Restart Device screen.

Parameter Description

- **Restart Device**: Restart the switch from within this screen. After restart, the switch will boot normally.
- **Buttons**:
  - Yes: Click and the device will restart.
  - No: Click to close this screen.

5.2 Firmware

This section describes how to upgrade firmware. The switch can be enhanced with more value-added functions by installing firmware upgrades.

5.2.1 Firmware Upgrade

This page facilitates an update of the firmware controlling the switch.

Web Interface

To configure a Firmware Upgrade Configuration in the Web interface:

1. Navigate within the Browser to select firmware in your device.

2. Click "Upload."

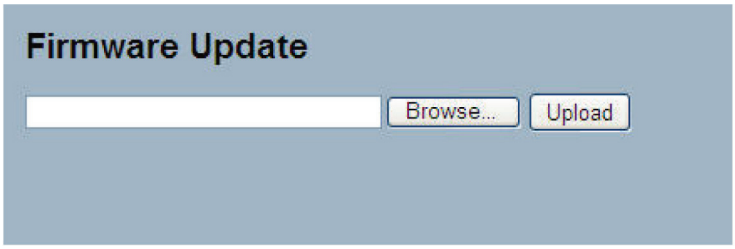


Figure 5-2. The Firmware Update screen

Parameter Description

- **Browse**: Click the "Browse..." button to search the firmware URL and filename.
- **Upload**: Click the "Upload" button. The switch will start to upload the firmware from files stored locally or on the server.

NOTE: This page facilitates an update of the firmware controlling the switch. Uploading software will update all managed switches to the location of a software image and click. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and all managed switches restart. Then the managed switch restarts.

WARNING: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

5.2.2 Firmware Selection

The switch supports dual images for firmware redundancy. You can select the firmware image for your device: Start firmware or Operating firmware. This page provides information about the active and alternate (backup) firmware images in the device, and enables you to revert to the alternate image.

Web Interface

To configure a Firmware Selection in the Web interface:

1. Click "Activate Alternate Image."
2. Click "OK" to complete firmware selection.

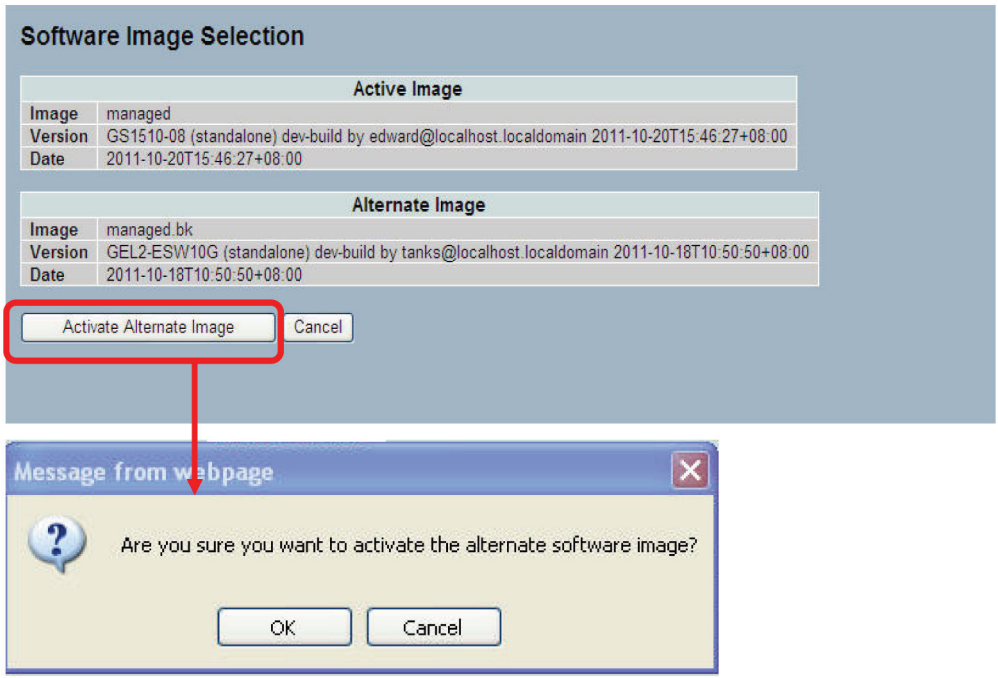


Figure 5-3. The Firmware Selection screen.

Parameter Description

- **Activate Alternate Image**: Click to use the alternate image. This button may be disabled depending on system state.
- **Cancel**: Cancel activating the backup image. Navigates away from this page.
- **Image**: The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk.
- **Version**: The version of the firmware image.
- **Date**: The date when the firmware was produced.

NOTE: In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.

NOTE: If the alternate image is active (because of a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.

NOTE: The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

5.3 Save / Restore

This section describes how to save and restore the switch configuration including reset to Factory Defaults, Save Start, Save Users, Restore Users for any maintenance needs.

5.3.1 Factory Defaults

This section describes how to reset the Switch configuration to Factory Defaults. Any configuration files or scripts will recover to factory default values.

Web Interface

To configure a Factory Defaults Configuration in the Web interface:

1. Click Factory Defaults.
2. Click Yes.

Figure 5-4. The Factory Defaults screen.

Parameter Description

- Buttons:
  - Yes: Click and the device will restart.
  - No: Click to close this screen.

5.3.2 Save Start

This section describes how to save the Switch Start configuration. Any current configuration files will be saved as XML format.

Web Interface

To configure a Save Start Configuration in the Web interface:

1. Click "Save Start."
2. Click "Yes."

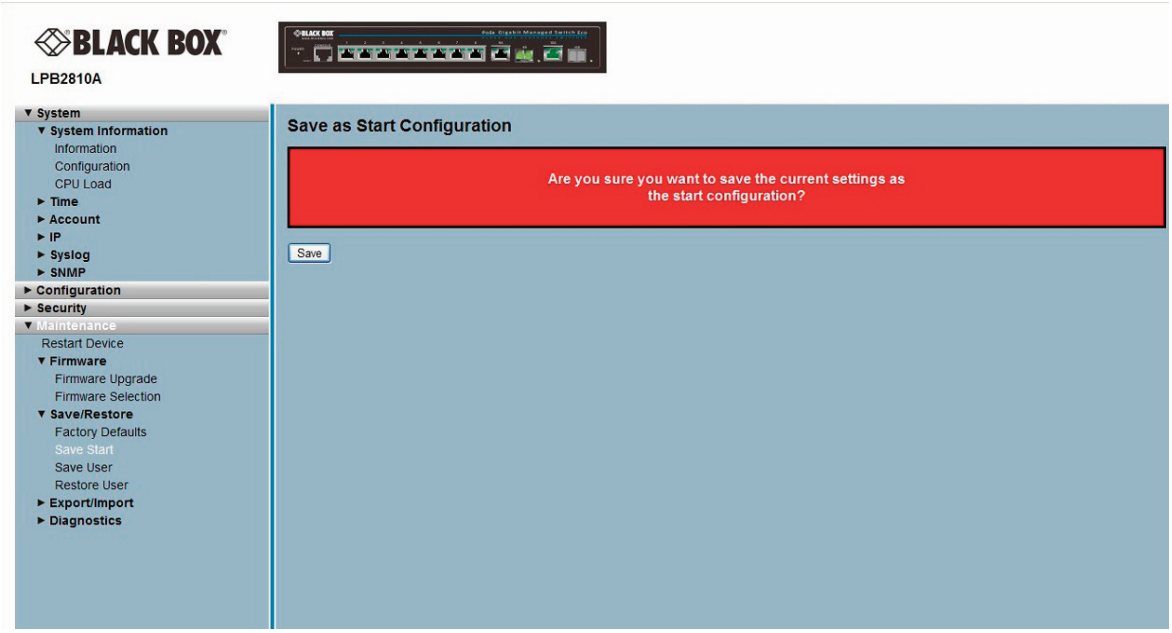


Figure 5-5. The Save Start configuration screen.

Parameter Description

- Buttons:
  - Save: Click to save changes.

5.3.3 Save User

This section describes how to save users' information. Any current configuration files will be saved as XML format.

Web Interface

To configure a Save User Configuration in the Web interface:

1. Click "Save User."
2. Click "Yes."

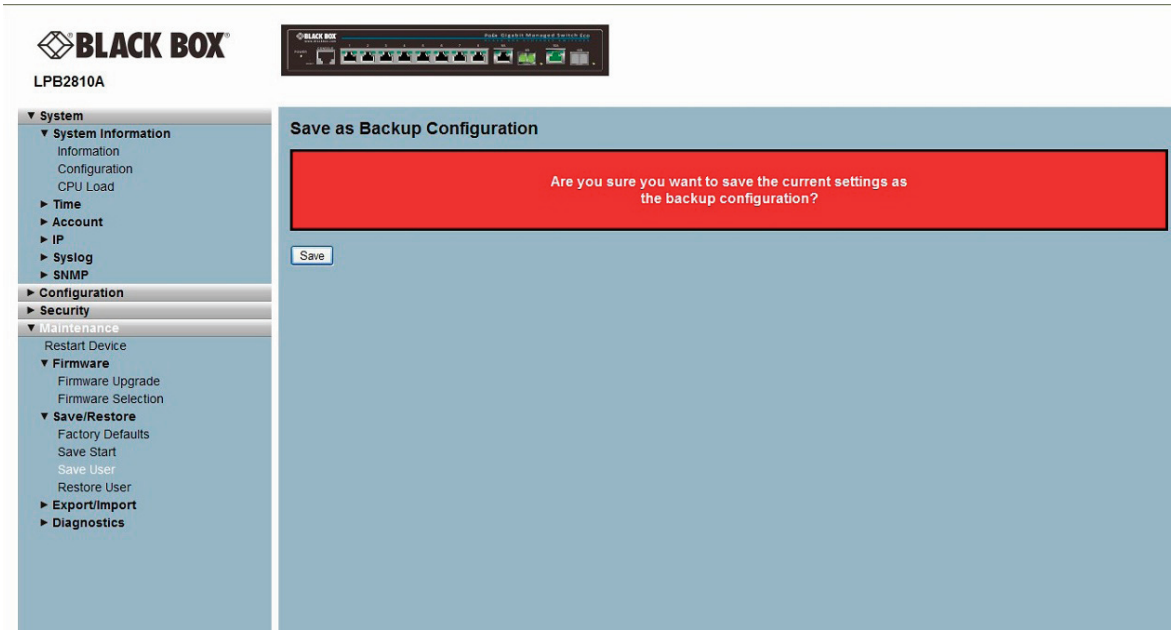


Figure 5-6. The Save as Backup Configuration screen.

Parameter Description

- Buttons:
  - Save: Click to save changes.

5.3.4 Restore User

This section describes how to restore user information back to the switch. Any current configuration files will be restored via XML format.

Web Interface

To configure a Restore User Configuration in the Web interface:

1. Click "Restore User."
2. Click "Yes."

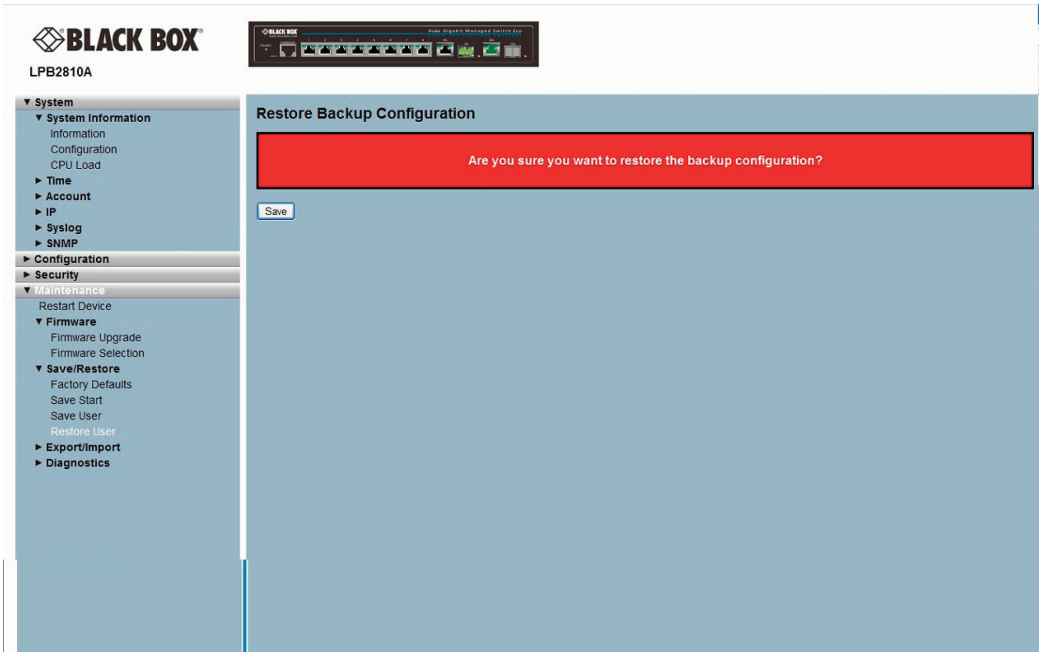


Figure 5-7. The Restore Backup Configuration screen.

Parameter Description

- Buttons:
  - Save: Click to save changes.

5.4 Export / Import

This section describes how to export and import the switch configuration. Any current configuration files will be exported as XML format.

5.4.1 Export Config

This section describes how to export the switch configuration for maintenance needs. Any current configuration files will be exported as XML format.

Web Interface

To configure a Export Config Configuration in the Web interface:

1. Click "Save configuration."
2. Save the file in your device.

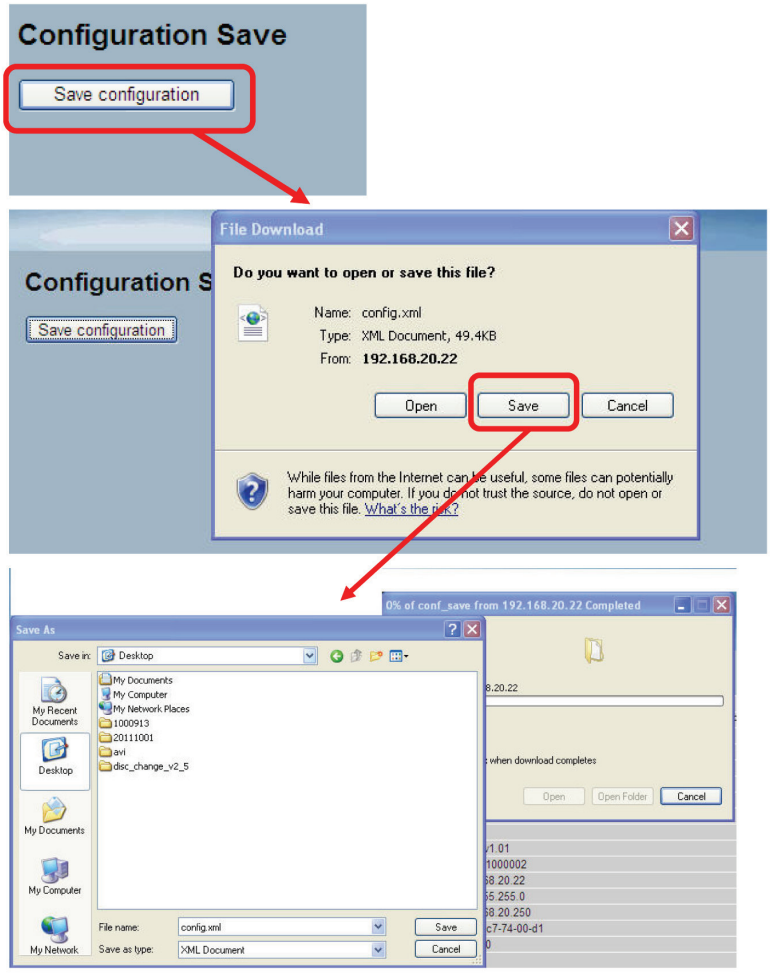


Figure 5-8. The Export Backup Configuration screen

Parameter Description

- **Buttons**:
  - Save: Click to save changes.

5.4.2 Import Config

This section describes how to import the switch configuration for maintenance needs. Any current configuration files will be imported as XML format.

Web Interface

To configure an Import Configuration in the Web interface:

1. Click "Browser to select the config file in your device."
2. Click "Upload."

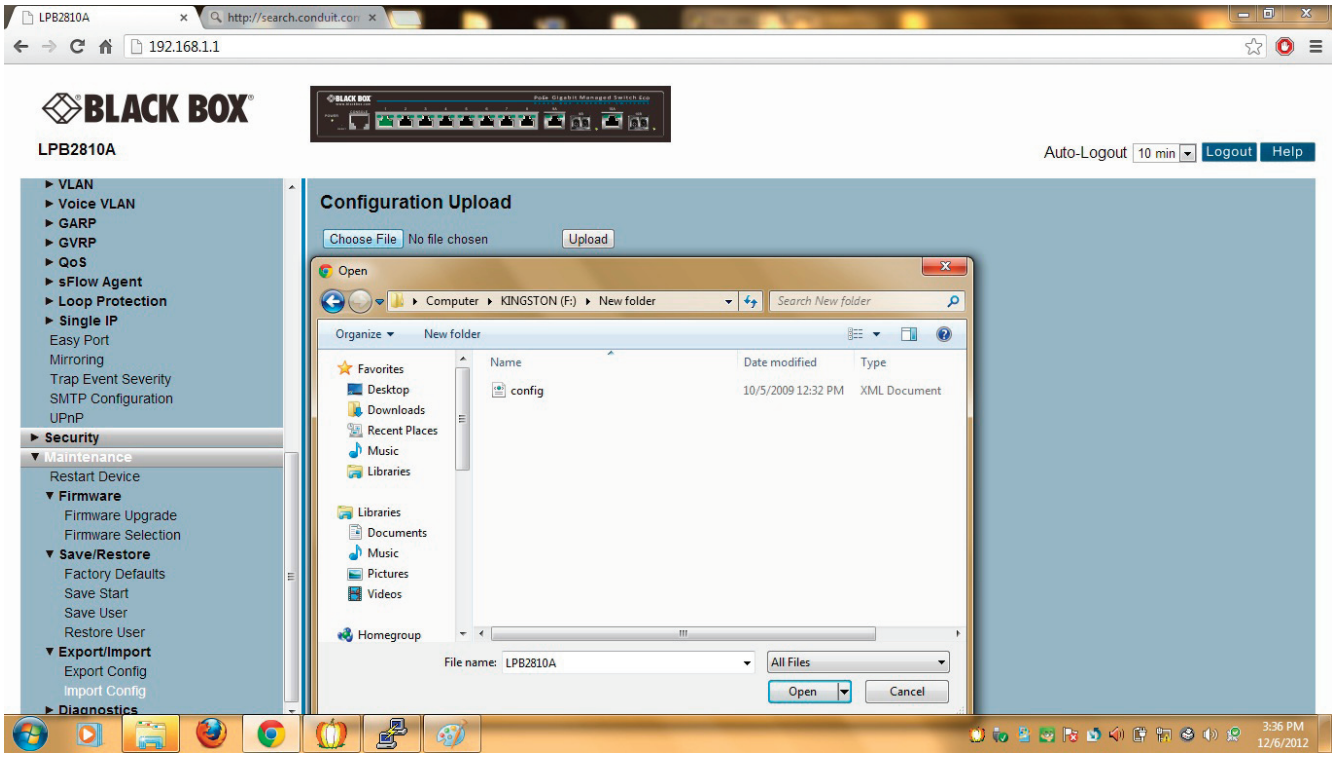


Figure 5-9. The Import Configuration screen.

Parameter Description

- **Browse**: Click the "Browse..." button to search the Configuration URL and filename.
- **Upload**: Click the "Upload" button. The switch will start to upload the configuration from the configuration stored locally in the PC or Server.

5.5 Diagnostics

This section provides a set of basic system diagnotsics. It lets users know that whether the system is healthy or needs to be fixed. The basic system check includes ICMP Ping, ICMPv6, and VeriPHY Cable Diagnostics.

5.5.1 Ping

This section allows you to issue ICMP PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMP PING Configuration in the Web interface:

1.Specify ICMP PING IP Address.

2.Specify ICMP PING Size.

3.Click "Start."

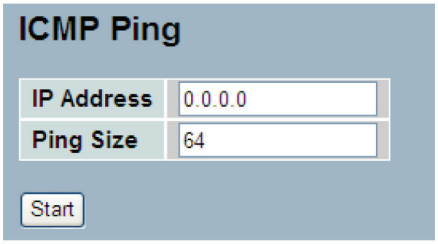


Figure 5-10. The ICMP Ping screen.

Parameter Description

- **IP Address**: To set the IP address of the device to ping.
- **Ping Size**: To set the ICMP packet size to ping the other device.
- **Start**: Click the "Start" button. The switch will start to ping the device using ICMP packet size set on the switch.

  After you click "Start," 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

  PING server ::10.10.132.20

  64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms

  64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms

  64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms

  64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms

  64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms

  Sent 5 packets, received 5 OK, 0 bad

5.5.2 Ping6

This section enables you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

Web Interface

To configure an ICMPv6 PING Configuration in the web interface:

1.Specify ICMPv6 PING IP Address.

2.Specify ICMPv6 PING Size.

3.Click "Start."

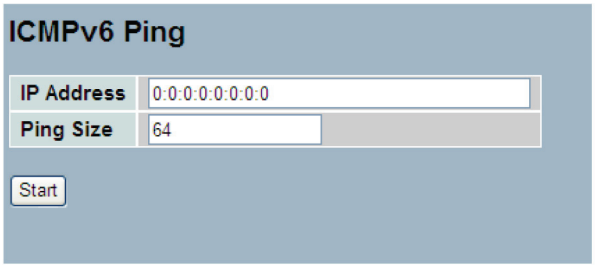


Figure 5-11. The ICMPv6 Ping screen.

Parameter Description

- **IP Address**: The destination IP Address with IPv6.
- **Ping Size**: The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.
- **Start**: Click the "Start" button. The switch will start to ping the device using the ICMPv6 packet size set in the "Ping Size" entry that has been set.

  After pressing "Start," five ICMPv6 packets will be transmitted. The sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

  PING6 server 10.10.132.20

  64 bytes from 10.10.132.20: icmp_seq=0, time=0ms

  64 bytes from 10.10.132.20: icmp_seq=1, time=0ms

  64 bytes from 10.10.132.20: icmp_seq=2, time=0ms

  64 bytes from 10.10.132.20: icmp_seq=3, time=0ms

  64 bytes from 10.10.132.20: icmp_seq=4, time=0ms

  Sent 5 packets, received 5 OK, 0 bad

5.5.3 VeriPHY

This section describes how to run the VeriPHY Cable Diagnostics. Press to run the diagnostics. It takes approximately five seconds to run. If all ports are selected, it can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of lengths between 30" and 459" (7–140 meters).

10- and 100-Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10- or 100-Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Web Interface

To configure a VeriPHY Cable Diagnostics Configuration in the Web interface:

1. Specify which port to check.
2. Click "Start."

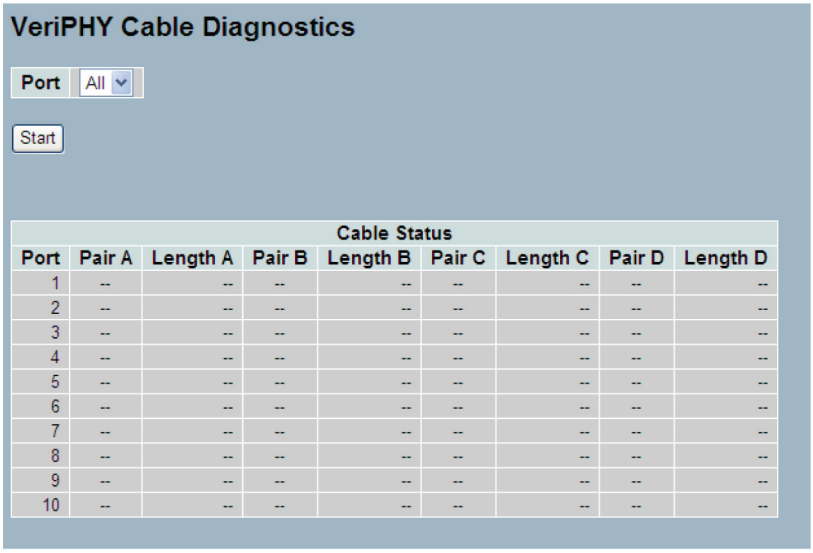


Figure 5-12. The VeriPHY Cable Diagnostics screen.

Parameter Description

- **Port**: The port where you are requesting VeriPHY Cable Diagnostics.
- **Cable Status**: Port: Port number.

  Pair: The status of the cable pair.

  Length: The length (in meters) of the cable pair.

Appendix: Glossary of Web-Based Management Terms

ACE: ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL: ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are three Web pages associated with the manual ACL configuration:

ACL|Access Control List: The Web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" Web page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" page. You can also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will only apply though if the frame gets past the ACE matching without getting matched. In that case, a counter associated with that port is incremented. See the Web page help text for each specific port property.

ACL|Rate Limiters: Under this page, you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1–1024K packets per seconds. Under "Ports" and "Access Control List" Web pages, you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES: AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

APS: APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation: Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability. (See also Port Aggregation, Link Aggregation.)

ARP: ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection: ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Autonegotiation: Autonegotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

CC: CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM: CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.

CDP: CDP is an acronym for Cisco Discovery Protocol.

DEI: DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES: DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations, which are based on a binary number called a key.

DHCP: DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay: DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies.

Specifically the option works by setting two suboptions: Circuit ID (option 1) and Remote ID (option 2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal to the DHCP relay agent's MAC address.

DHCP Snooping: DHCP Snooping is used to block an intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS: DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS: DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or a network connection, an attacker may be able to prevent network users from accessing e-mail, Web sites, on-line accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation: Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets. An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP: DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

EEE: EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS: EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type: Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

FTP: FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave: Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

HTTP: HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (Port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS: HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provides authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses Port 443 instead of HTTP Port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

ICMP: ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic, or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions.

IEEE 802.1X: IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP: IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for on-line video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier: A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP: IMAP is an acronym for Internet Message Access Protocol. It is a protocol for e-mail clients to retrieve e-mail messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your e-mail messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP: IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an Internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the network.

The current version of the Internet protocol is IPv4, which has 32-bit Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of Webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bit Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC: IPMC is an acronym for IP MultiCast.

IP Source Guard: IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

LACP: LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

LLC: The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1-byte DSAP (Destination Service Access Point), 1-byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP: LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by that management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED: LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LOC: LOC is an acronym for Loss Of Connectivity and is detected by a MEP. It indicates lost connectivity in the network. Can be used as a switch criteria by EPS.

MAC Table: Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports. The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MD5: MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

MEP: MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

Mirroring: For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.) Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD: MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MVR: Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP) networks that enables multicast traffic from a source VLAN to be shared with subscriber VLANs. The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVRVLAN and forwarded to the VLANs where hosts have requested it/them.

NAS: NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS: NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN). The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS: NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems. NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP: NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

OAM: OAM is an acronym for Operation Administration and Maintenance. It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this Optional TLVs.

An LLDP frame contains multiple TLVs. For some TLVs it is configurable if the switch includes the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLV is disabled, the corresponding information is not included in the LLDP frame.

OUI: OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address, which forms the first 24 bits of a MAC address.

PCP: PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD: PD is an acronym for Powered Device. In a PoE system, the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY: PHY is an abbreviation for Physical Interface Transceiver. It is the device that implements the Ethernet physical layer (IEEE-802.3).

Ping: Ping is a program that sends a series of packets over a network or the Internet to a specific computer to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected. Ping uses Internet Control Message Protocol (ICMP) packets. The ping request is the packet from the origin computer, and the ping Reply is the packet response from the target.

PoE: PoE is an acronym for Power over Ethernet. PoE is used to transmit electrical power, to remote devices over standard Ethernet cable. It could, for example, be used for powering IP telephones, wireless LAN access points, and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer: A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3: POP3 is an acronym for Post Office Protocol version 3. It is a protocol for e-mail clients to retrieve e-mail messages from a mail server. POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server. POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

Private VLAN: In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP: PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

QCE: QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and ag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL: QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects. Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL: QL In SyncE this is the Quality Level of a given clock source. This is received on a port in an SSM indicating the quality of the clock received in the port.

QoS: QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

RARP: RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS: RADIUS is an acronym for Remote Authentication Dial-n User Service. It is a networking protocol that provides centralized access, authorization, and accounting management for people or computers to connect and use a network service.

RDI: RDI is an acronym for Remote Defect Indication. It is an OAM functionallity that is used by a MEP to indicate a defect detected to the remote peer MEP.

RSTP: In 1998, with document 802.1w, the IEEE introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

SHA: SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper: A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP: SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP: The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more

protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP: SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMPs allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP: SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as a transport layer.

SSID: Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one.

SSH: SSH is an acronym for Secure Shell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality.

SSM: SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP: Spanning Tree Protocol is an OSI Layer 2 protocol that ensures a loop-free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

SyncE: SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network "clock frequency" synchronized. Not to be confused with real-time clock synchronized (IEEE 1588).

TACACS+: TACACS+ is an acronym for Terminal Acess Controller Access Control System Plus. It is a networking protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services.

Tag Priority: Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP: TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers. The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host. The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET: TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TFTP: TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

UDP: UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers. UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact. Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

User Priority: User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

VLAN: Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID: VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN: Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

Black Box Tech Support: FREE! Live. 24/7.

Great tech support is just 30 seconds away at 724-746-5500 or blackbox.com.

BLACK BOX®
NETWORK SERVICES

About Black Box

Black Box provides an extensive range of networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech Support available in 30 seconds or less.

© Copyright 2012. Black Box Corporation. All rights reserved.

LPB2810A, Rev 1